



Phishing Campaign

May 2024

IR-2024-05-04-01

Executive Summary

- On May 4, 2024, a threat actor conducted a phishing email campaign against USC email accounts.
- These emails collected contact, demographic, and occupation data for future compromises or to attempt to scam users.
- The campaign used a previously observed method to avoid automated threat detection by embedding malicious links into Word document attachments.

Beginning May 4, an unidentified threat actor began a phishing campaign against USC email accounts. This campaign consisted of ~220,000 emails from 236 unique Gmail addresses with Word document attachments that contained links to Google Forms. These forms, masquerading as job applications, solicited contact, demographic, and occupation information from victims. This is a similar methodology to a known threat actor, although the novel use of Word documents precludes a definitive correlation. This method has been observed on a smaller scale in a prior campaign by potentially the same threat actor.

Recommendations

- **IR-2024-05-04-01-R1:** Continue automating phishing email detection and remediation. Automation brings the mean time to detect (MTTD) and the mean time to remediate (MTTR) closer to real-time, reducing the amount of time users are exposed to the threat.

IR-2024-05-04-01 – Docx Phishing Campaign

Threat Actor Methods

The Malicious Emails

The threat actor sent over 200,000 emails on Saturday May 4, 2024. This was a strategic time for them to attack, as graduation was occurring at the time the emails were sent. Initiating a campaign during an important campus event increases the chance of the threat actor's actions going undetected for longer. The threat actor possibly also sought to take advantage of new graduates who will be looking for a job after graduation. This makes them more likely to open the attachment and provide their information.

The malicious emails had an eye-catching subject line, usually in all capital letters, with no body text. Attached to the emails were documents with the intended message. This tactic is commonly used by threat actors to avoid automated anti-phishing detection.



Figure 1. Phishing email with the malicious attachment.

The email attachments were Microsoft Word Document Files (docx) describing a potential part-time job offer. Recipients interested were encouraged to apply using the Google Form link provided. The links were not hyperlinked, making them not clickable in the document and forcing the user to copy and paste the link into their browser to access it. This tactic is often used to further avoid detection, as Microsoft Defender logs when a user has clicked a link in Microsoft Outlook.

Personal Assistant Service

All Email recipients Staff/Students are encouraged to be a part of this amazing offer. This is a part time job that will not affect your present employment or study at the campus & you'll be working from home. It's fun, rewarding, and flexible.

2-3 hours daily

Three Hundred And Fifty Dollars (\$450)

Part-Time

Note ; Only 17+ Above


To apply Copy and paste this(forms.gle/7o4QrAkyrqaghNUW8)

Figure 2. Contents of Word document attachment with the malicious Google Form link.

The Google Form

The forms solicited the following personal information from the user:

- Full name
- Personal email address
- University email address
- Home address
- Phone number
- Occupation
- Age



PERSONAL ASSISTANT

You have been offered a Job Opportunity at the convenience of your home or school, Which serve as a gateway to pay expenses incurred on campus. This opportunity should be done at leisure taking at most 3hrs/day, 2-3 times a week and earn \$495 Weekly. It's a Flexible Opportunity where you will determine your working time. All the tasks are work from home/on campus job, you don't need to travel somewhere and also you don't need to have a car to get started. It's an home base office work you can be in any location and work from your home/school.

JOB RESPONSIBILITIES MAY INCLUDE, BUT NOT LIMITED TO:-

- Running Personal errands-
- Organization, scheduling day to day activities, and coordinating travel plans-
- Paying strict attention to detail and takes detailed notes-
- Assist with general official errands, support and assistance with various administrative tasks and project as needed

This position will be home-based and flexible part time job, You can be working from home, School or any location

BENEFITS:

- AD & D Insurance.
- 401(k). (After 3 months with us, plus an increase in your weekly paycheck).
- Free medicals. (After 1 months with us, plus an increase in your weekly paycheck)

jack.stavrakas@gmail.com [Switch account](#)

Not shared

* Indicates required question

FULL NAME *

Your answer

Figure 3. Malicious Google Form.

Many Unique Addresses

Instead of sending their attempts through one or a small group of addresses, the threat actor chose to bombard the email client with over 200 unique Gmail addresses. The email addresses appear to be automatically generated with a loose template of a first and last name, followed by three numbers. Since Gmail accounts are free, the threat actor could implement an automated process to create many accounts without any monetary cost. This makes blocking each address impractical, as more email accounts can be created faster than the old ones can be blocked. Multiple emails have been observed sending the same file, which makes blocking the unique file hash the most practical and efficient option.

Automatically generating email accounts on a large scale also allows the threat actor to send an overwhelming number of emails without setting off spam filters. Most spam detection is designed to detect one email address sending many emails at one time. However, if there are over fifty emails sending a smaller number of emails at one time, they become more difficult to detect and remediate without preparing for that scenario.

50 of the email addresses were randomly sampled and are shown in Appendix A.

Comparison to Previous Campaigns

The threat actor followed a similar pattern to a smaller scale campaign the Security Operations team responded to in February 2024. The threat actor used PDF files as their attachments instead of the Word documents seen here. Over 50 unique Gmail addresses were used in the previous incident. Due to the similarities in the emails delivered in both instances, it is possible that both incidents had the same threat actor.

Detection

Overview

The Security Operations team was notified of the phishing campaign on Saturday, May 4, 2024, at 8:46 am by the team's automated phishing detection application. The application logs emails reported to the phishing mailbox and notifies the Security Operations team if the number of reported emails with the same subject exceeds a set threshold. The application made additional reports between 9:12 am and 1:05 pm.

The Phishing Bot

The Automated Phishing Detection Bot (known as "Phishing Bot") is an automated detection tool used to detect potential phishing campaigns and notify the Security Operations team. The bot is developed using Microsoft Power Automate, a tool used to automate processes within Microsoft applications. Phishing Bot takes in messages from the Phishing mailbox, organizes them into a Microsoft SharePoint list. The bot then looks for repeated subject lines. When a subject line is repeated enough times, the Security Operations team is notified, and manual investigation is initiated.

Incident Response

Search and Purge

Once aware of the campaign in progress, the Security Operations team collected the SHA256 hashes of the email attachments and used those to soft delete (move to the Deleted Items folder) the emails and block any future emails sent with the file attachments. The URLs that led to the Google Forms found in Figure 2 and Appendix C were also added to the Defender Tenant Add/Block List (TABL).

Investigation

Threat Actor Statistics and Information

- The phishing emails were delivered from 236 unique Gmail addresses.
 - A random sample of 50 of the addresses are available in Appendix A.
- 928 emails were delivered from a single address on average.
 - 23 subject lines were observed during the original incident. A full list is available in Appendix B.
- Only 3 unique attachments were seen in the 218,923 emails that were initially sent.

Current Status

The Security Operations team monitored other emails sent from the threat actor several days after the initial incident.

1. On May 6, 2024, new emails were sent from the threat actor that had three file attachments not seen in the previous wave: COAST.docx, ESSENTIAL.docx, and PREVIEW NOW.docx.
2. On May 7, 2024, new emails were sent with one new attachment: Folder.docx.
3. On May 10, 2024, another set of emails were sent with one new attachment: Notice.docx.
4. On May 12, 2024, the threat actor sent out a Microsoft PowerPoint attachment titled ASSIGNMENT.pptx containing the fake job offer.

Each of these documents followed the same format as the others shown in Figure 2 and Appendix C.

The emails were soft-deleted using Microsoft Defender, and the SHA256 file hashes for each attachment were used to block future emails. The Security Operations team is continuing to monitor phishing reports to quickly detect and remediate any further phishing attempts from this threat actor.


Appendix A. Table of sender addresses and counts.

Sender Address	Count
klueverschnackel239@gmail.com	979
annarinopeacher559@gmail.com	975
lahayestcharles277@gmail.com	974
kolkowskiybarro839@gmail.com	974
drahotaangilletta386@gmail.com	968
parlinterh326@gmail.com	965
uphoffpostell458@gmail.com	963
causbysadorra542@gmail.com	960
hassettchea901@gmail.com	959
jonesmillet823@gmail.com	958
klutemy0@gmail.com	956
duelnewbrough17@gmail.com	956
phodelina369@gmail.com	956
libbietetdy216@gmail.com	954
hebeisenascher823@gmail.com	953
heenatrattner982@gmail.com	953
wolmanlaye630@gmail.com	952
ferguswuerz186@gmail.com	951
charriervalcho325@gmail.com	950
venneridyas922@gmail.com	949
holmsteadsegers831@gmail.com	949
saunierhauenstein266@gmail.com	948
manlykillary647@gmail.com	944
costerenshaw277@gmail.com	943
pingreyhennings865@gmail.com	943
dallmanreon939@gmail.com	942
lecontelukesh601@gmail.com	942
rusinmclay890@gmail.com	935
riflekempainen613@gmail.com	934
candrastendeback333@gmail.com	933
hamperbirtcher927@gmail.com	933
boddekerricklefs884@gmail.com	933
hamleygriffen81@gmail.com	932
casperscunio632@gmail.com	932
hollenbergbrocker687@gmail.com	932
engelsbourland866@gmail.com	928
barociovillaneuva397@gmail.com	927
koutrasmirra19@gmail.com	926
termeerlankster156@gmail.com	921
reigelnamey856@gmail.com	917
henkehuter386@gmail.com	916
gougeosako944@gmail.com	914
barzeysandness506@gmail.com	878
mabeealbino629@gmail.com	814

Appendix B. Table of subject lines and counts.

Subject	Count
ACCORD	77964
APPLY NOW	37330
APPPLY NOW	4726
ATTENTION	9341
CONCLUDE	907
CONFIRM	1853
CONFIRMING	8105
CONNECTING	13079
Efficiency	7713
EXCITING	10344
FW: APPLY NOW	144
NOME-BASED WORK	5137
INVOLVE	928
LOOKOUT	5612
NEW HIRE	7535
NEW HIRING	943
ON GOING OFFER	962
PERMIT	1884
RECOMMEND	9349
REFERRAL	10342
South Carolina Students Offer	949
WORK ACCEPTANCE	928
WORK FROM HOME	2848

Appendix C. Extended samples of observed Google Forms and Word documents.



PERSONAL ASSISTANT

You have been offered a Job Opportunity at the convenience of your home or school, Which serve as a gateway to pay expenses incurred on campus. This opportunity should be done at leisure taking at most 3hrs/day;2-3 times a week and earn \$495 Weekly. It's a Flexible Opportunity where you will determine your working time. All the tasks are work from home/on campus job, you don't need to travel somewhere and also you don't need to have a car to get started. It's an home base office work you can be in any location and work from your home/school.

JOB RESPONSIBILITIES MAY INCLUDE, BUT NOT LIMITED TO:-

- Running Personal errands
- Organization, scheduling day to day activities, and coordinating travel plans
- Paying strict attention to detail and takes detailed notes
- Assist with general official errands, support and assistance with various administrative tasks and project as needed

This position will be home-based and flexible part time job, You can be working from home, School or any location

BENEFITS:
AD & D Insurance.
401(k). (After 3 months with us, plus an increase in your weekly paycheck).
Free medicals. (After 1 months with us, plus an increase in your weekly paycheck)

jack.stavrakas@gmail.com [Switch account](#)

Not shared

* indicates required question

FULL NAME *

Your answer

PERSONAL EMAIL (NOT YOUR SCHOOL EMAIL ADDRESS) *

Your answer

SCHOOL EMAIL *

Your answer

HOME ADDRESS

Your answer

PHONE NUMBER

Your answer

OCCUPATION

Your answer

AGE


Your answer

[Submit](#) [Clear form](#)

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

Google Forms



DATEBASE INFORMATION

You have been offered a Job Opportunity at the convenience of your home or school, pay expenses serve as a gateway to pay expenses incurred on campus. This opportunity should be done at leisure taking at most 3hrs/day;2-3 times a week and earn \$495 Weekly. It's a Flexible Opportunity where you will determine your working time. All the tasks are work from home/on campus job, you don't need to travel somewhere and also you don't need to have a car to get started. It's an home base office work you can be in any location and work from your home/school.

JOB RESPONSIBILITIES MAY INCLUDE, BUT NOT LIMITED TO:-

- Running Personal errands
- Organization, scheduling day to day activities, and coordinating travel plans
- Paying strict attention to detail and takes detailed notes
- Assist with general official errands, support and assistance with various administrative tasks and project as needed

This position will be home-based and flexible part time job, you can be working from home, School or any location

BENEFITS:
AD & D Insurance.
401(k). (After 3 months with us, plus an increase in your weekly paycheck).
Free medicals. (After 1 months with us, plus an increase in your weekly paycheck)

jack.stavrakas@gmail.com [Switch account](#)

Not shared

FULL NAME

Your answer

PERSONAL EMAIL (NOT YOUR SCHOOL EMAIL ADDRESS)

Your answer

SCHOOL EMAIL

Your answer

HOME ADDRESS

Your answer

PHONE NUMBER

Your answer

OCCUPATION

Your answer

AGE

Your answer

[Submit](#) [Clear form](#)

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

Google Forms

Personal Assistant Service

All Email recipients Staff/Students are encouraged to be a part of this amazing offer. This is a part time job that will not affect your present employment or study at the campus & you'll be working from home. It's fun, rewarding, and flexible.

2-3 hours daily

Four Hundred And Fifty Dollars (\$450)

Part-Time Job

Note ; Only 17+ Above

To apply Copy and paste this()

Personal Assistant Service

All Email recipients Staff/Students are encouraged to be a part of this amazing offer. This is a part time job that will not affect your present employment or study at the campus & you'll be working from home. It's fun, rewarding, and flexible.

2-3 hours daily

Three Hundred And Fifty Dollars (\$450)

Part-Time

Note ; Only 17+ Above

To apply Copy and paste this()