Binghamton University, Watson School of Engineering

Phishing in Focus: Examining Exploits
(Detection)

(Lokesh Sesham - B00969886)
Science of Cyber Security – CS559-01
Prof. Guanhua Yan
10/23/2023

Contents

1. Setting Up Environment

1.1. Introduction

Phishing attacks are now a pervasive threat in the digital world, impacting individuals , business, and organizations. This project explores methods to detect and combat these malicious activities. It's important to address the commonality of phishing attacks, driven by a lack of awareness, and provide insights into prevention.

In this project , I took help from SET to construct a Facebook phishing page, which creates a replica of the genuine login page of the Facebook website. Facilitated by Ngrok, a secure tunneling service, we establish a connection between the fake page and our system. Unwriting victims interact with this page, and their provided credentials are discreetly captured. By comprehending these techniques, individuals and organizations can bolster their defenses against such deceptive practices.

This project is structured into many key sections , each will address distinct aspects of phishing detection. We emphasize that while these detection techniques and tools are powerful, no system is infallible , and some phishing emails may still bypass these filters.

1.2. Overview

This project dives into the world of phishing attacks, which are a common form of online deception that tricks people into sharing sensitive information by exploiting their trust. We're using Kali Linux, a powerful open-source computer system , along with the Social Engineering Toolkit(SET), to create a fake Facebook login page. The goal is to show how this is done, the tools used, and the steps involved, all to capture the login details of unsuspecting individuals .

We can use a secure service called Ngrok to create a connection between the fake page and the attacker's system. This allows us to secretly collect login information when people interact with fake page. The main purpose of this project is to let everyone know how phishing works and so they can be safe and protect themselves in this digital world.

1.3. Host Virtual Machine

The virtual machine serves as the environment for executing the phishing attack. The Virtual platform is Kali Linux, a purpose-built Linux distribution meticulously crafted for penetration testing also known as pen testing and ethical hacking purposes. Kali Linux comes with a preconfigured array of the security testing tools and software. And for hosting the phishing website and its respective database, specific packages need to be installed within the Kali Linux system.

2. Detection Strategies

As my project is on Phishing attacks, there are many possible ways to detect this attack.

2.1. URL Analysis: Employ URL analysis tools or services to check the legitimacy of website links in emails or messages.

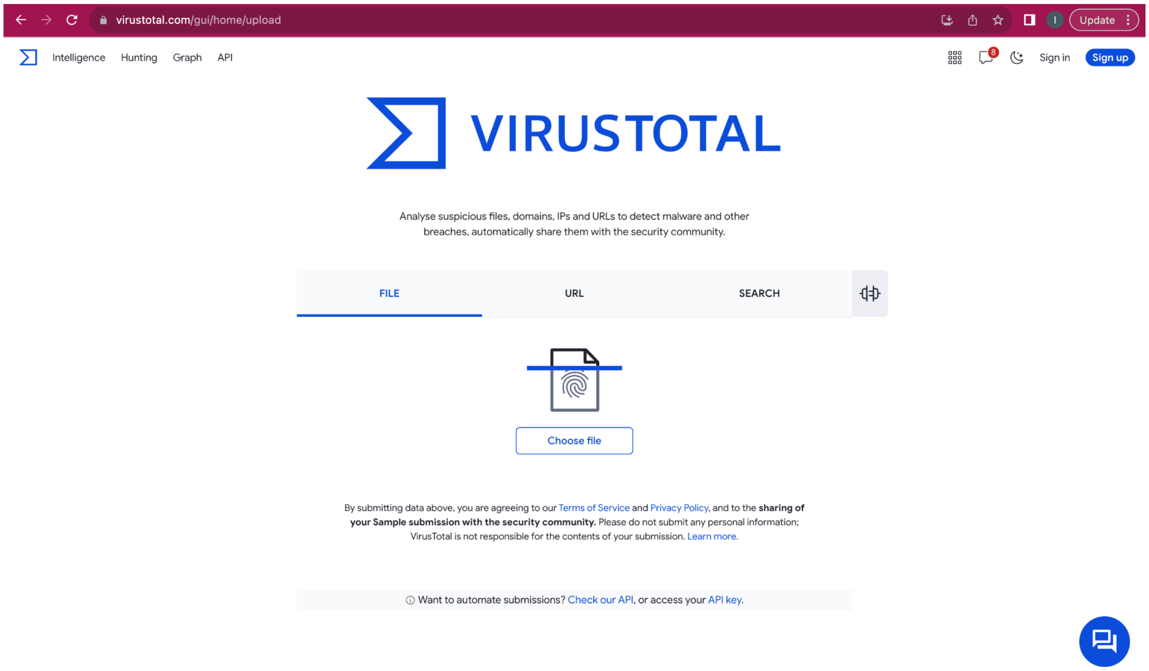
2.2. Look for indicators such as misspellings, unusual characters, or variations in the domain name that may suggest a phishing attempt.
2.3. Anti-phishing Link detection.
2.4. Security incident Monitoring.
2.5. Email Filters and Spam Detection.

2.1. URL Analysis

URL Analysis is a process which helps to identify and mitigate phishing attacks. Phishing is a malicious practice where attackers attempt to deceive individuals into revealing sensitive information, such as passwords, by impersonating legitimate websites and services. Analyzing attempts and taking appropriate precautions. The main aspects of URL analysis are:

1. **Domain Spoofing:** Phishing attackers often create URLs that mimic legitimate domain names to trick users into believing they are visiting a trusted website. In some cases we can analyze the domain name in a URL which helps us to find some misspellings, extra characters, or suspicious variations that indicate a spoofed domain.
2. **Subdomain Analysis:** Phishers can use subdomains to make their URL appear more legitimate. Analyzing subdomains can help identify inconsistencies or unexpected subdomains that are not typically associated with the legitimate website.
3. **SSL Certification:** phishers can use SSL Certificates to make their Fake website appear secure. However, analyzing the SSL certificate can reveal discrepancies or irregularities that indicate a phishing attempt. Users should look for SSL certificate errors and warnings, Such as mismatched domain names or expired certificates.
4. **URL Redirection:** Phishers frequently use URL redirection techniques to hide the true destination of a link. Analyzing the URL for multiple redirects or suspicious redirection patterns that can help find potential phishing attempts.
5. **URL Shorteners:** Phishers use URL shortening services to mask the true destination of a link. Analyzing the expanded URL behind a shortened link can help uncover the actual website being linked to and assess its legitimacy.

So for this URL Analysis, we can also use a website : https://www.virustotal.com/gui/home/upload.
With this website, you can test a URL and as well as a file with which you can confirm that the link and the pdf is phishing or not.
The website looks like this-

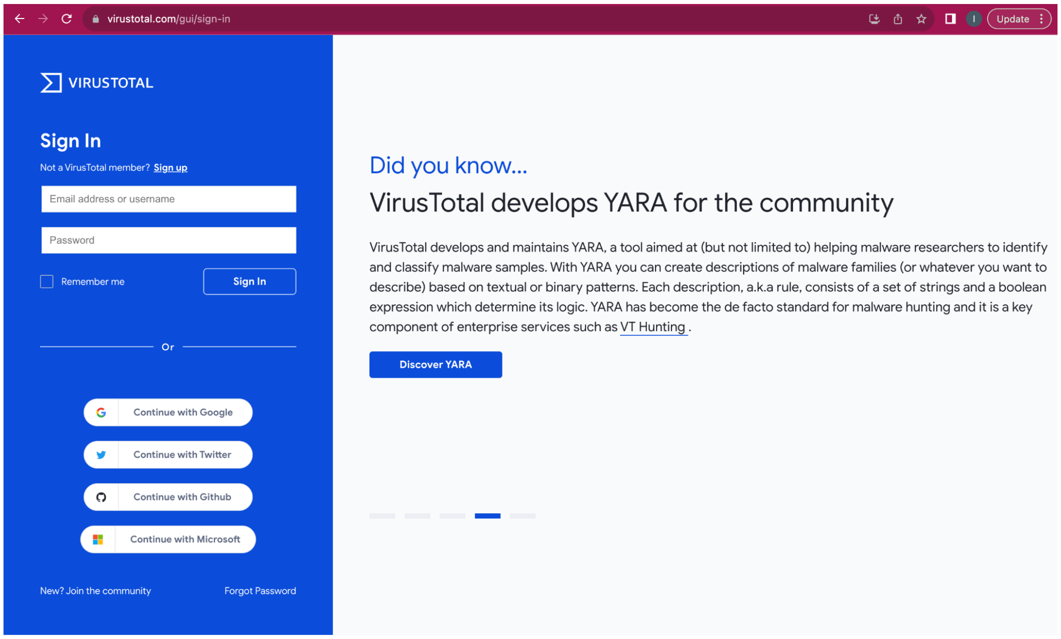


Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, or access your API key.

- Sign in to the website with a mail id.

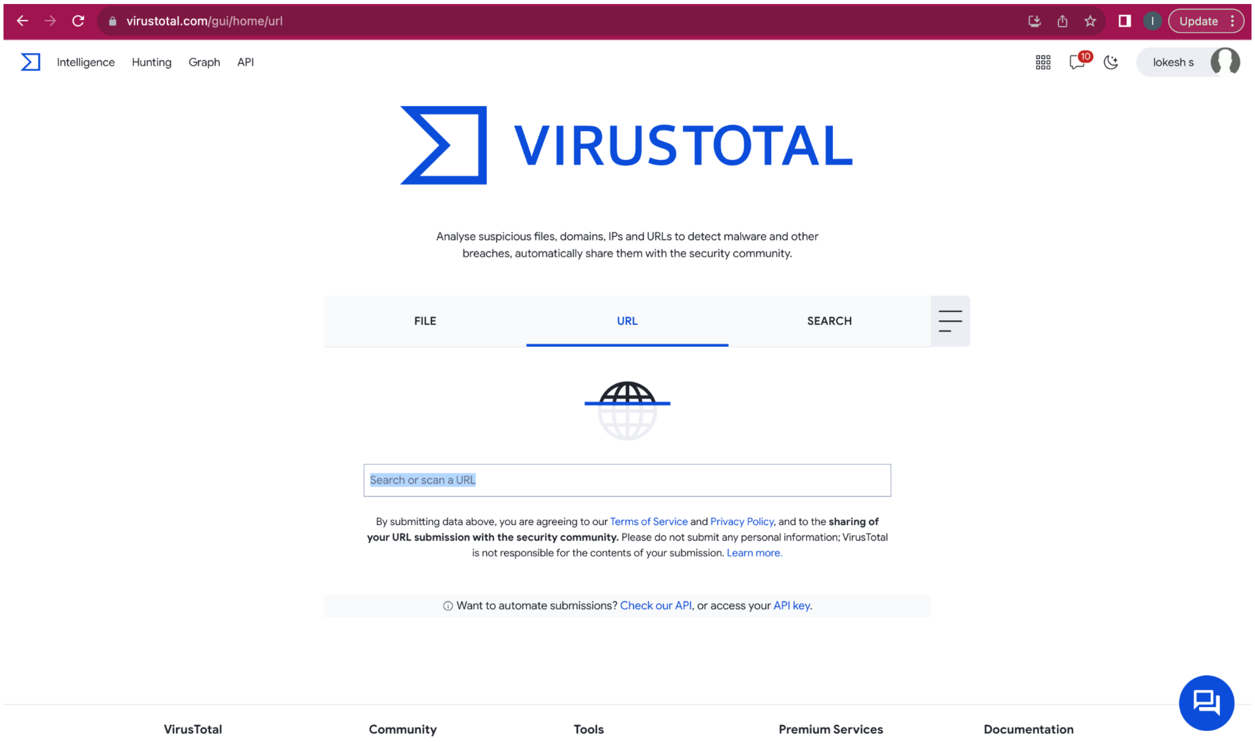


Did you know...

VirusTotal develops YARA for the community

VirusTotal develops and maintains YARA, a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns. Each description, a.k.a rule, consists of a set of strings and a boolean expression which determine its logic. YARA has become the de facto standard for malware hunting and it is a key component of enterprise services such as VT Hunting .

- And copy the link that you want to test and confirm whether it is a phishing link or not.



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your URL submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

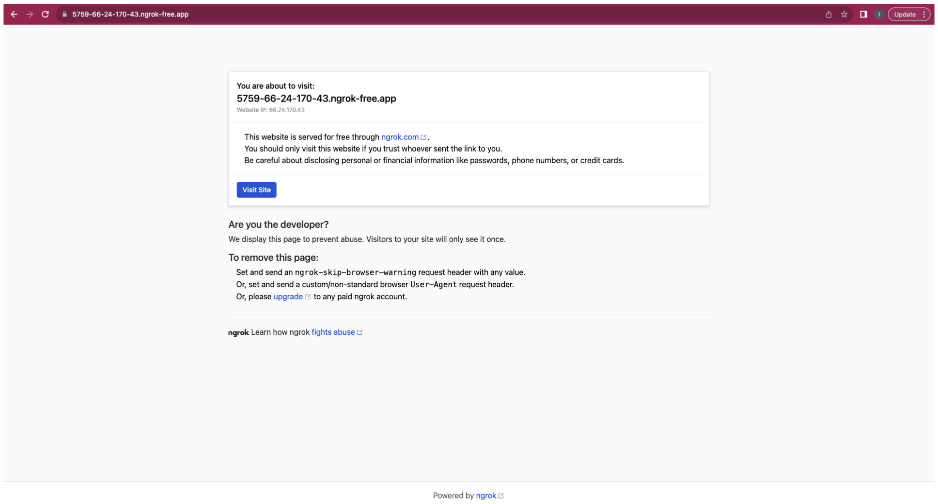
Want to automate submissions? Check our API, or access your API key.

- So here is the phishing link that I got in my first project

> https://5759-66-24-170-43.ngrok-free.app/
> 5759-66-24-170-43.ngrok-free.app

which looks like a facebook login page. It happens in two steps

1. As it appears in the below image



You are about to visit:
5759-66-24-170-43.ngrok-free.app
Website IP: 66.24.170.43

This website is served for free through ngrok.com.
You should only visit this website if you trust whoever sent the link to you.
Be careful about disclosing personal or financial information like passwords, phone numbers, or credit cards.

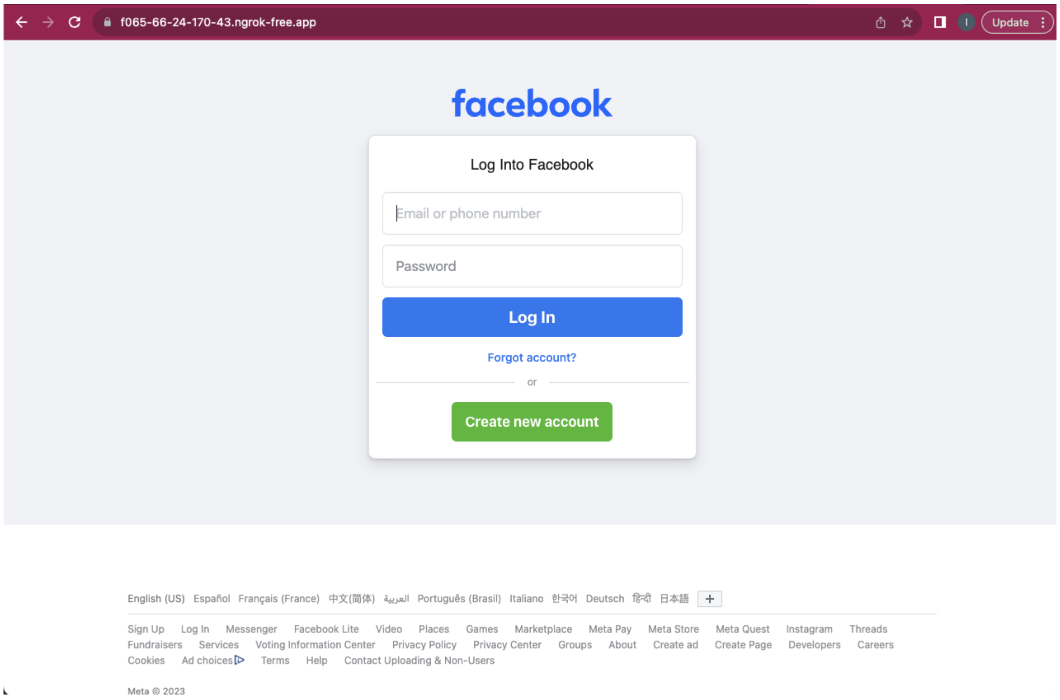
Are you the developer?
We display this page to prevent abuse. Visitors to your site will only see it once.

To remove this page:
Set and send an `ngrok-skip-browser-warning` request header with any value.
Or, set and send a custom/non-standard browser `User-Agent` request header.
Or, please upgrade to any paid ngrok account.

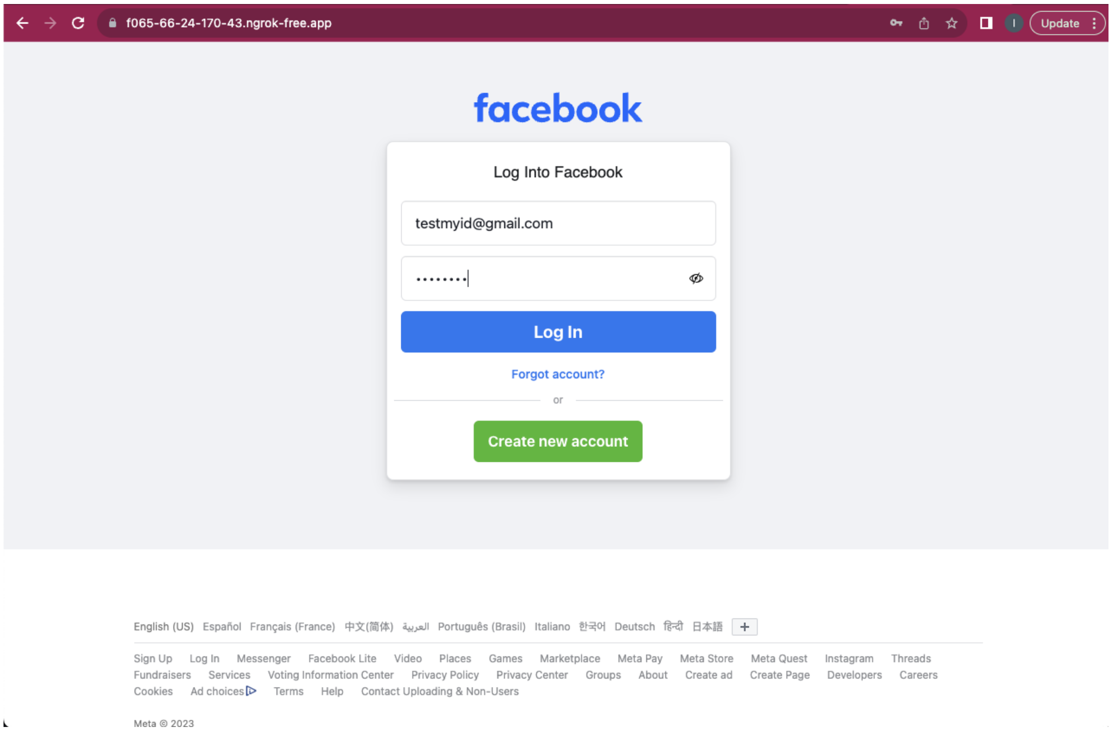
ngrok Learn how ngrok fights abuse

Powered by ngrok

2. And when I hit the “visit site” prompt , It redirects me to the Facebook login page. where that is not the original facebook page, it was just the Fake Facebook login page that I created with the help of SET, Kali Linux and Ngrok. Where the fake facebook page looks like this .


f065-66-24-170-43.ngrok-free.app
Update
facebook
Log Into Facebook
Email or phone number
Password
Log In
Forgot account?
or
Create new account
English (US) Español Français (France) 中文(简体) العربية Português (Brasil) Italiano 한국어 Deutsch हिन्दी 日本語 +
Sign Up Log In Messenger Facebook Lite Video Places Games Marketplace Meta Pay Meta Store Meta Quest Instagram Threads
Fundraisers Services Voting Information Center Privacy Policy Privacy Center Groups About Create ad Create Page Developers Careers
Cookies Ad choices Terms Help Contact Uploading & Non-Users
Meta © 2023

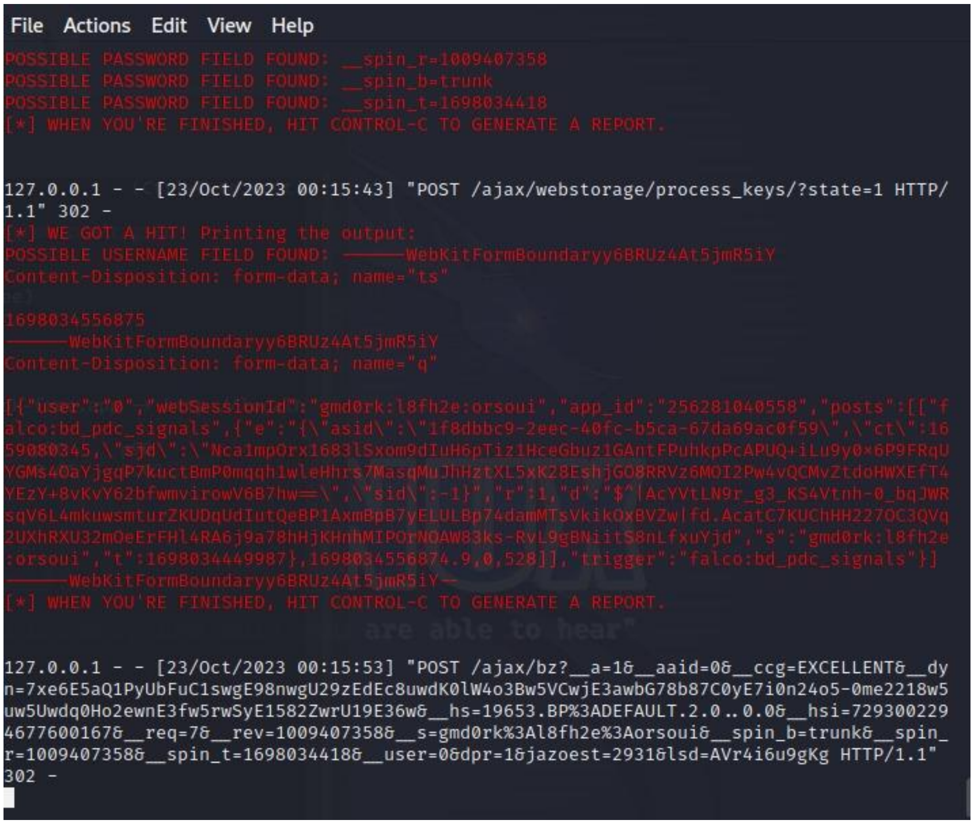
- And When I will be entering my credentials, like this


f065-66-24-170-43.ngrok-free.app
Update
facebook
Log Into Facebook
Log In
Forgot account?
or
Create new account
English (US) Español Français (France) 中文(简体) العربية Português (Brasil) Italiano 한국어 Deutsch हिन्दी 日本語 +
Sign Up Log In Messenger Facebook Lite Video Places Games Marketplace Meta Pay Meta Store Meta Quest Instagram Threads
Fundraisers Services Voting Information Center Privacy Policy Privacy Center Groups About Create ad Create Page Developers Careers
Cookies Ad choices Terms Help Contact Uploading & Non-Users
Meta © 2023

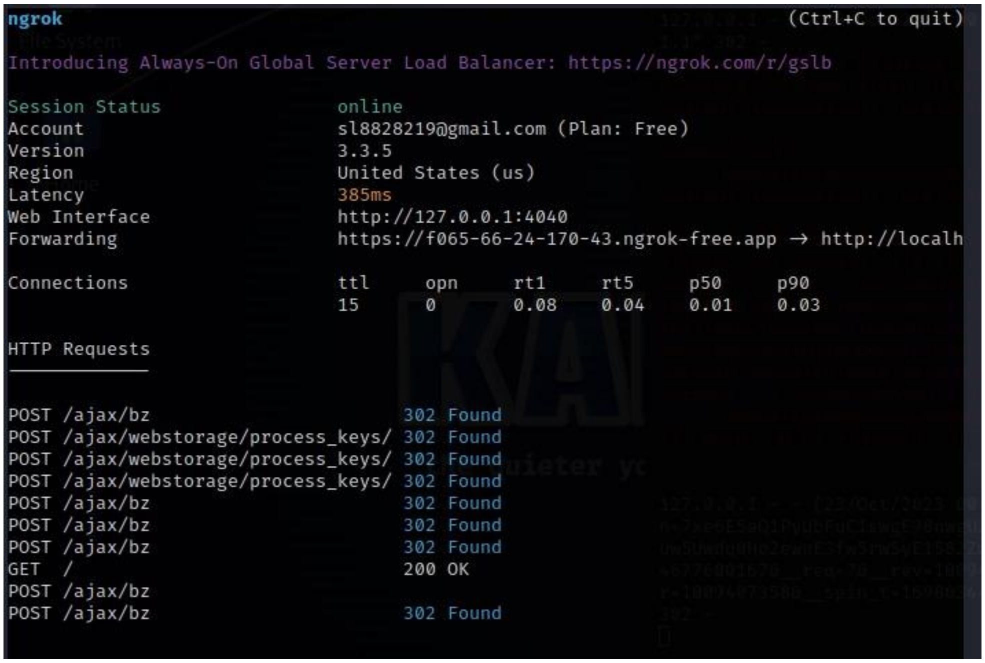
testmyid@gmail.com

••••••••

- I will be getting the credentials in the kali Linux terminal,

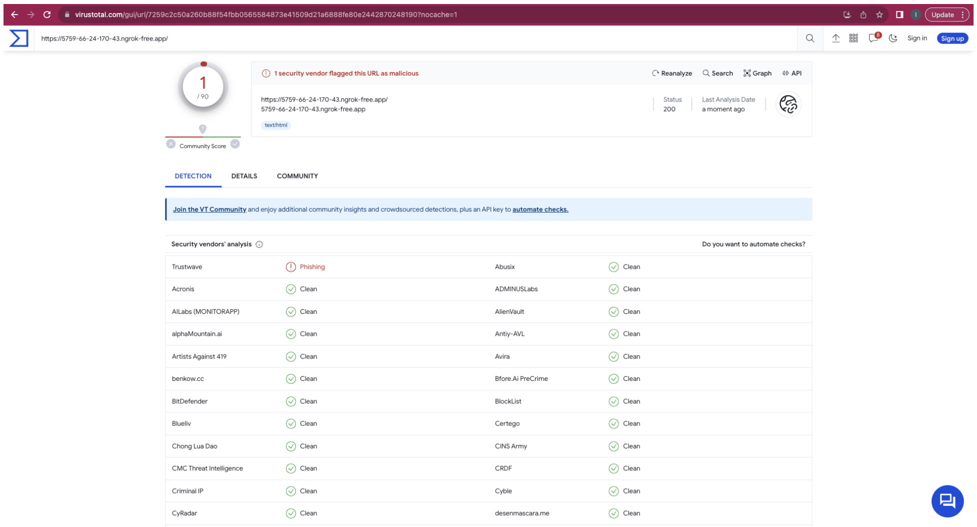


```
POSSIBLE PASSWORD FIELD FOUND: __spin_r=1009407358
POSSIBLE PASSWORD FIELD FOUND: __spin_b=trunk
POSSIBLE PASSWORD FIELD FOUND: __spin_t=1698034418
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


127.0.0.1 - - [23/Oct/2023 00:15:43] "POST /ajax/webstorage/process_keys/?state=1 HTTP/
1.1" 302 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: ------WebKitFormBoundaryy6BRUz4At5jmR5iY
Content-Disposition: form-data; name="ts"

1698034556875
------WebKitFormBoundaryy6BRUz4At5jmR5iY
Content-Disposition: form-data; name="q"

[{"user":"0","webSessionId":"gmd0rk:l8fh2e:orsoui","app_id":"256281040558","posts":[["f
alco:bd_pdc_signals",{"e":"{\"asid\":\"1f8dbbc9-2eec-40fc-b5ca-67da69ac0f59\",\"ct\":16
59080345,\"sjd\":\"Nca1mpOrx1683lSxom9dIuH6pTiz1HceGbuz1GAntFPuhkpPcAPUQ+iLu9y0×6P9FRqU
YGMs4OaYjgqP7kuctBmP0mqqh1wleHhrs7MasqMuJhHztXL5xK28EshjGO8RRVz6MOI2Pw4vQCMvZtdoHWXEfT4
YEzY+8vKvY62bfwmvirowV6B7hw==\",\"sid\":-1}","r":1,"d":"$^|AcYVtLN9r_g3_KS4Vtnh-0_bqJWR
sqV6L4mkuwsmturZKUDqUdIutQeBP1AxmBpB7yELULBp74damMTsVkikOxBVZw|fd.AcatC7KUChHH227OC3QVq
2UXhRXU32mOeErFHl4RA6j9a78hHjKHnhMIPOrNOAW83ks-RvL9gBNiitS8nLfxuYjd","s":"gmd0rk:l8fh2e
:orsoui","t":1698034449987},1698034556874.9,0,528]],"trigger":"falco:bd_pdc_signals"}]
------WebKitFormBoundaryy6BRUz4At5jmR5iY--
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


127.0.0.1 - - [23/Oct/2023 00:15:53] "POST /ajax/bz?__a=1&__aaid=0&__ccg=EXCELLENT&__dy
n=7xe6E5aQ1PyUbFuC1swgE98nwgU29zEdEc8uwdK0lW4o3Bw5VCwjE3awbG78b87C0yE7i0n24o5-0me2218w5
uw5Uwdq0Ho2ewnE3fw5rwSyE1582ZwrU19E36w&__hs=19653.BP%3ADEFAULT.2.0..0.0&__hsi=729300229
4677600167&__req=7&__rev=1009407358&__s=gmd0rk%3Al8fh2e%3Aorsoui&__spin_b=trunk&__spin_
r=1009407358&__spin_t=1698034418&__user=0&dpr=1&jazoest=2931&lsd=AVr4i6u9gKg HTTP/1.1"
302 -
```



```
ngrok                                                                   (Ctrl+C to quit)

Introducing Always-On Global Server Load Balancer: https://ngrok.com/r/gslb

Session Status                online
Account                       sl8828219@gmail.com (Plan: Free)
Version                       3.3.5
Region                        United States (us)
Latency                       385ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    https://f065-66-24-170-43.ngrok-free.app -> http://localh

Connections                   ttl     opn     rt1     rt5     p50     p90
                              15      0       0.08    0.04    0.01    0.03

HTTP Requests
-------------

POST /ajax/bz                          302 Found
POST /ajax/webstorage/process_keys/    302 Found
POST /ajax/webstorage/process_keys/    302 Found
POST /ajax/webstorage/process_keys/    302 Found
POST /ajax/bz                          302 Found
POST /ajax/bz                          302 Found
POST /ajax/bz                          302 Found
GET  /                                 200 OK
POST /ajax/bz
POST /ajax/bz                          302 Found
```

And this is the Phishing link I have got from my terminal(https://f065-66-24-170-43.ngrok-free.app) , where if someone opens this link and enters their credentials, I can get their credentials . But now my task is to show the detection of the phishing link. So, I will paste this link in the website: https://www.virustotal.com/gui/home/upload and clearly get the information about the link and finally we will get to know that the link I pasted is a phishing link.



virustotal.com/gui/url/7259c2c50a260b88f54fbb0565584873e41509d21a6888fe80e2442870248190?nocache=1

https://5759-66-24-170-43.ngrok-free.app/

1 security vendor flagged this URL as malicious

https://5759-66-24-170-43.ngrok-free.app/
5759-66-24-170-43.ngrok-free.app
text/html

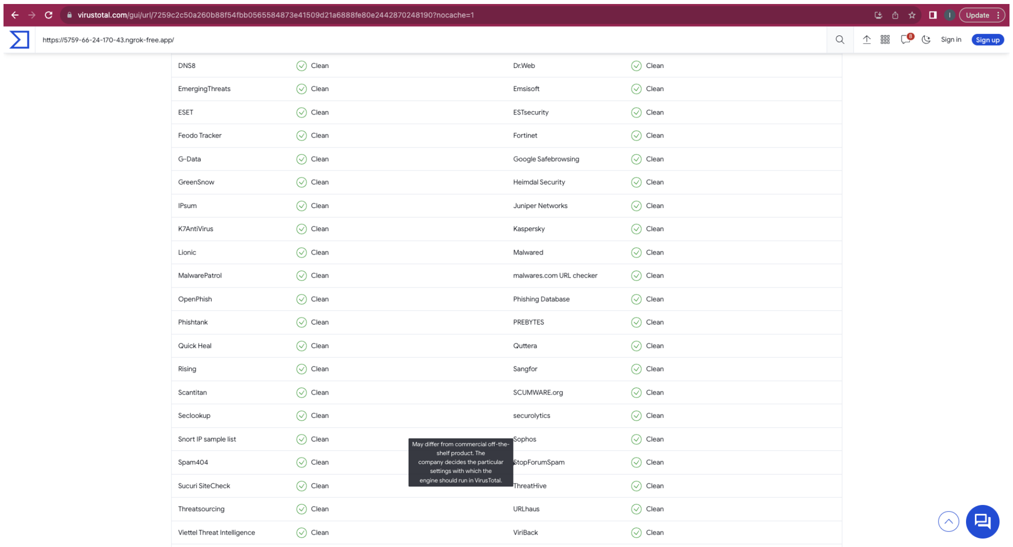
Status 200
Last Analysis Date a moment ago

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

Security vendors' analysis

Do you want to automate checks?

Trustwave	Phishing	Abusix	✓ Clean
Acronis	✓ Clean	ADMINUSLabs	✓ Clean
AILabs (MONITORAPP)	✓ Clean	AlienVault	✓ Clean
alphaMountain.ai	✓ Clean	Antiy-AVL	✓ Clean
Artists Against 419	✓ Clean	Avira	✓ Clean
benkow.cc	✓ Clean	Bfore.Ai PreCrime	✓ Clean
BitDefender	✓ Clean	BlockList	✓ Clean
Blueliv	✓ Clean	Certego	✓ Clean
Chong Lua Dao	✓ Clean	CINS Army	✓ Clean
CMC Threat Intelligence	✓ Clean	CRDF	✓ Clean
Criminal IP	✓ Clean	Cyble	✓ Clean
CyRadar	✓ Clean	desenmascara.me	✓ Clean



virustotal.com/gui/url/7259c2c50a260b88f54fbb0565584873e41509d21a6888fe80e2442870248190?nocache=1

https://5759-66-24-170-43.ngrok-free.app/

DNS8	✓ Clean	Dr.Web	✓ Clean
EmergingThreats	✓ Clean	Emsisoft	✓ Clean
ESET	✓ Clean	ESTsecurity	✓ Clean
Feodo Tracker	✓ Clean	Fortinet	✓ Clean
G-Data	✓ Clean	Google Safebrowsing	✓ Clean
GreenSnow	✓ Clean	Heimdal Security	✓ Clean
IPsum	✓ Clean	Juniper Networks	✓ Clean
K7AntiVirus	✓ Clean	Kaspersky	✓ Clean
Lionic	✓ Clean	Malwared	✓ Clean
MalwarePatrol	✓ Clean	malwares.com URL checker	✓ Clean
OpenPhish	✓ Clean	Phishing Database	✓ Clean
Phishtank	✓ Clean	PREBYTES	✓ Clean
Quick Heal	✓ Clean	Quttera	✓ Clean
Rising	✓ Clean	Sangfor	✓ Clean
Scantitan	✓ Clean	SCUMWARE.org	✓ Clean
Seclookup	✓ Clean	securolytics	✓ Clean
Snort IP sample list	✓ Clean	Sophos	✓ Clean
Spam404	✓ Clean	StopForumSpam	✓ Clean
Sucuri SiteCheck	✓ Clean	ThreatHive	✓ Clean
Threatsourcing	✓ Clean	URLhaus	✓ Clean
Viettel Threat Intelligence	✓ Clean	ViriBack	✓ Clean

May differ from commercial off-the-shelf product. The company decides the particular settings with which the engine should run in VirusTotal.

- So this is the URL Analysis process , with this we can get to know that the link is original ,safe and secure or we can also know whether the link is fake, scam and harmful.

2.2. Indicators of Phishing Attempts

- When it comes to identifying potential phishing attempts, it is important to check for the indicators that can help distinguish legitimate websites from fraudulent ones.

1. **Misspellings:** Phishers often create URLs with intentionally misspelled domain names to trick users that make them believe they are visiting the legitimate website. They may replace some letters with similar looking characters or add extra letters. For example, instead of “paypal.com”, a phishing URL might use “paypa1.com” or “paypaal.com”. So by carefully examining the domain name for any misspellings, users can spot potential phishing attempts.

2. **Unusual Characters:** The URLs that a phisher sends may include unusual characters or symbols that are not typically found in legitimate domain names. These characters can be used to mimic letters or deceive users. To explain in detail a phishing URL might use a Crrillic “a” instead of latin (a) in a domain like “bankofamerica.com”. Being vigilant and watching out for such unusual characters may help to identify potential phishing attacks.
3. **Variations in the Domain Name:** Phishers often create domain names that similarly look like popular websites or services. They may add “hyphens”, “numbers” or additional words to the domain name. For example, a phishing URL might use “faceb00k-login.com” instead of the legitimate “ facebook.com”. By comparing the domain name in the URL to the known legitimate domain , users can detect variations that may indicate a phishing attempt.

2.3. Anti-phishing Link detection

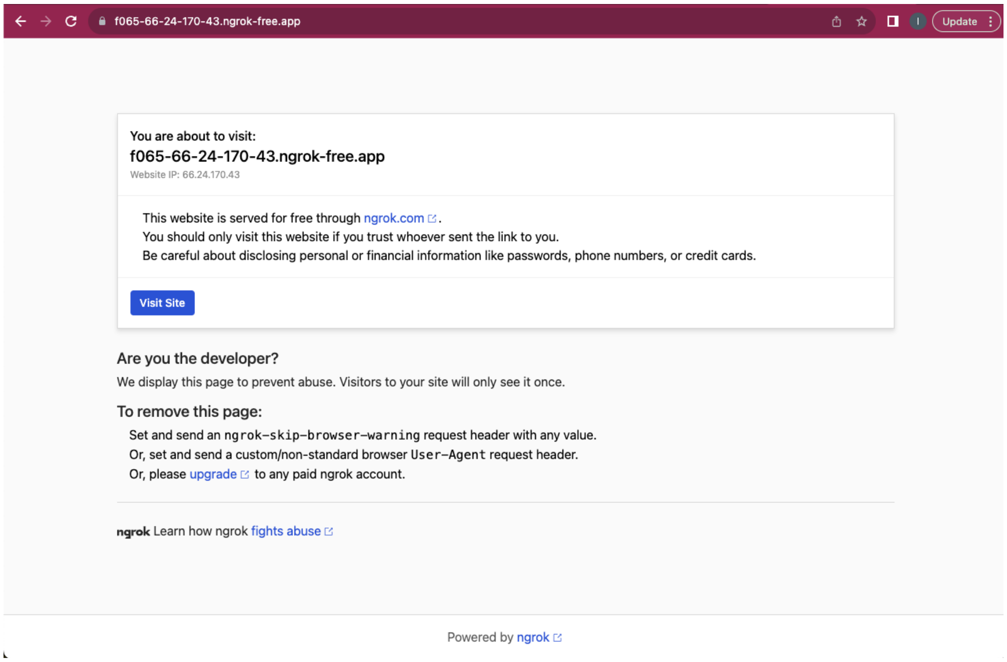
Anti-phishing software is designed to detect and prevent phishing attacks by identifying and blocking malicious links or websites. This provides an additional layer of protection against phishing attempts, complementing other security measures such as email filters and user awareness. And coming to anti-phishing software:

1. **Link Analysis:** Anti-phishing software uses advanced algorithms and databases to analyze URLs and determine if they are associated with known phishing attacks. It also compares the URL against a database of known phishing sites or uses real-time analysis to assess the legitimacy of the link. If a link is found as suspicious and malicious, the software can block access to the website or display a warning to the user. Example : Trend Micro Internet Security Software.
2. **Website reputation:** Anti-phishing software depends on the reputation based systems to assess the trustworthiness of the websites. It keeps the database of known legitimate websites and known phishing sites. When a User clicks on a link, the software checks the website’s reputation against this database. If the website is flagged as suspicious or has a poor reputation, and the software blocks all the access and displays a warning. Example : Kaspersky Internet Security.
3. **Phishing Email Detection:** This software also helps for this project “Phishing in focus: examining exploits” . Some anti-phishing software integrates with email clients to scan incoming emails for phishing attempts. It analyzes the content, links, and attachment within emails to identify potential phishing attacks. If a malicious or suspicious mail is detected, the software can quarantine the mail, mark it as spam, or display a warning to the user.

2.4. Security incident Monitoring

1. Detection: Security incident monitoring involves the use of various tools, technologies, and techniques which help to detect the phishing attacks. Which includes monitoring network traffic, analyzing email patterns, and finding threat intelligence feeds to identify suspicious activities or indicators of phishing attempts.

- From 2.1. URL analysis , when I copied the URL (that I got from Kali Linux terminal), and pasted it in my browser , the first this I got is an alert from my browser like this:



You are about to visit:

f065-66-24-170-43.ngrok-free.app

Website IP: 66.24.170.43

This website is served for free through ngrok.com.
You should only visit this website if you trust whoever sent the link to you.
Be careful about disclosing personal or financial information like passwords, phone numbers, or credit cards.

Visit Site

Are you the developer?

We display this page to prevent abuse. Visitors to your site will only see it once.

To remove this page:

Set and send an `ngrok-skip-browser-warning` request header with any value.
Or, set and send a custom/non-standard browser `User-Agent` request header.
Or, please upgrade to any paid ngrok account.

ngrok Learn how ngrok fights abuse

Powered by ngrok

Generally , when we open any original link (like www.facebook.com) , the above message doesn't prompt this alert. This alert we got is because of two reasons. One is we have Phishing Filters and Safe browsing that every browser contains and also there are some other features we should go through (like anti-phishing extensions) in our browser and add them to our browser extensions. This helps us to be safe, secure and alert with every link that we open.

2. **Phishing Filters:** Browsers can incorporate phishing filters that analyze web pages and emails for known phishing indicators. These filters can identify suspicious links, deceptive content, or malicious attachments commonly associated with phishing attacks. If a phishing email is found , and to detect that , the browser can flag it as a threat or move to the spam folder.

2.5. Email Filters and Spam Detection

Email Filters and spam detection are very important as these play a key factor for identifying and blocking phishing links in emails. This technology is designed to detect incoming emails, identify potential phishing attempts. As mentioned in 2.3 , Link analysis is also one of the major part in Email filters and spam detection.

1. **Content analysis:** Email filters and spam detection systems use content analysis techniques to identify the content of incoming emails. They find different aspects of elements such as the email subject, sender, body text, and embedded links to find out potential phishing indicators. This analysis helps in detecting suspicious and malicious links that may lead to phishing websites.
2. **Machine learning and AI:** Advanced email filters utilize machine learning and Artificial intelligence algorithms to continuously improve their phishing detection capabilities. These algorithms learn from patterns and characteristics of known phishing emails, links and allows them to find latest and evolving phishing techniques. This adaptive approach helps in detecting previously unseen phishing links.
3. **User Feedback and Reporting :** Email filters frequently incorporate mechanisms for users to provide feedback on suspicious phishing emails. Users can report suspicious emails, include those

containing phishing links, which helps to improve the effectiveness of the email filter. This feedback from the users helps other users in refining the detection algorithms and enhancing the overall security of the email system.

- Here we should note one point , no system is perfect. And some phishing emails can still bypass these filters.

3. Table Of Confusion

Statement	**True Positive**	**False Positive**	**False Negative**
URL Analysis	Yes	No	No
Look for Indicators	Yes	No	Yes
Anti-phishing link detection	Yes	No	Yes
Security incident monitoring	N/A	N/A	N/A
Email Filters and Spam detection	Yes	Yes	No

4. Conclusion

Phishing detection is a critical aspect of combating the ever-evolving threat landscape. This project has explored different detecting techniques and tools for phishing attempts. One such method is URL analysis , which involves scrutinizing web links for indicators of deception, such as misspellings or variations in domain names. With the mentioned techniques they can become more adept at identifying potential phishing URLs and avoiding falling victim to malicious schemes.

The other effective approach to phishing detection is the use of anti-phishing link detection software. This technology helps us to scan and analyze URLs to find and block the malicious links. With the help of machine learning algorithms and reputation based systems, these tools can detect patterns and characteristics linked with phishing attacks. This proactive measure adds an extra layer of protection, preventing users from accessing fake websites and inadvertently disclosing sensitive information.

Additionally, Security incident monitoring plays a crucial role in phishing detection. By employing advanced tools and technologies , organizations can monitor network traffic, analyze email patterns, and leverage threat intelligence feeds to identify suspicious activities or indicators of phishing attempts. This proactive approach allows security teams to detect and respond to phishing attacks in real-time, minimizing the potential impact on the users and systems.

Concluding this, effective phishing detection requires a combination of user awareness, technological solutions, and proactive monitoring. By educating users about phishing indicators, implementing anti-phishing link detection software, and employing security incident monitoring practices, organizations can enhance their ability to detect and mitigate phishing attacks. This multi-faceted approach is crucial in maintaining a secure digital environment and safeguarding against the ever-present threat of phishing.

6. Bibliography

1. https://blog.usecure.io/famous-phishing-attacks
2. https://www.virustotal.com/gui/home/upload
3. https://www.researchgate.net/publication/361283096_Analysis_of_Cyber_Security_Attacks_ using_Kali_Linux
4. http://www.cs.cmu.edu/~ponguru/pk_final_proposal.pdf
5. https://safebrowsing.google.com/
6. https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks
7. https://cofense.com/
8. https://www.ibm.com/topics/cybersecurity
9. https://learn.microsoft.com/en-US/microsoft-365/security/office-365-security/anti-spam-protection-about?view=o365-worldwide