CYBER THREAT INTELLIGENCE REPORT

Assignment 2 – Practical Assignment

SMS Attack

12/04/2022

A. D. DISSANAYAKA @00608177

a.d.dissanayaka@edu.salford.ac.uk

ABSTRACT

On December 3, 1992, the very first SMS message was sent across the Vodafone GSM network in the United Kingdom. In banking, government, and many other sectors, SMS (Short Message Service) is used as a vital communication platform. Nowadays, this is not a secure platform for sending any sensitive data, because its existing security mechanism cannot ensure protection from scamming, alteration, eavesdropping, or man-in-the-middle attacks.

This paper presents an overview of SMS attacks, the previous initiatives undertaken by researchers in terms of improving SMS security aspects, limitations, and recommendations to improve SMS security mechanisms. In order to identify loopholes and provide comprehensive solutions, a realistic attacking scenario was performed on a simulated Android smartphone through the Dagah platform.

1. INTRODUCTION

While the fast development and dissemination of Information and Communication Technology (ICT) are making people's lives easier, it is also posing severe challenges to society. In fact, mobile technology has advanced significantly. Due to the improved functionality and services available, mobile communication usage has increased drastically over the last two decades. Mobile phones are used for a variety of reasons, including staying in touch with family, conducting business, and having access to a phone in the event of an emergency. Social media access, international roaming (phone calls, text messages, and mobile data), the Short Message Service (SMS), and other cost-effective services (e.g., Mobile camera) are some of the most highlighted features of mobile phones in the present day. SMS has become the most popular of all the mobile telephony services.

SMS (Short Message Service) is a text messaging service available on most phones, computers, and mobile devices. It makes use of conventional communication protocols to allow mobile devices to send and receive short text messages. Text messaging may be a convenient, quick, and flexible way to increase communication while also nurturing connections and engagement. SMS malware is any malicious programme that is sent to users via text message. Today, cybercriminals are sending text messages that contain misleading information with links to fake websites or downloads that could cost you dearly if you fall for them. Malicious software and websites are used in these attacks to enact harm to users [1]. Among the many sorts of SMS attack threats, there are a few that stand out. They are SMS Phishing (Smishing), Mobile

Malware, and Premium-rate SMS scams. SMS phishing or "smishing" is when an attacker uses text messaging to impersonate a reputable person or institution in order to trick people into giving over their personal information (as illustrated in Figures 1, 2, and 3).

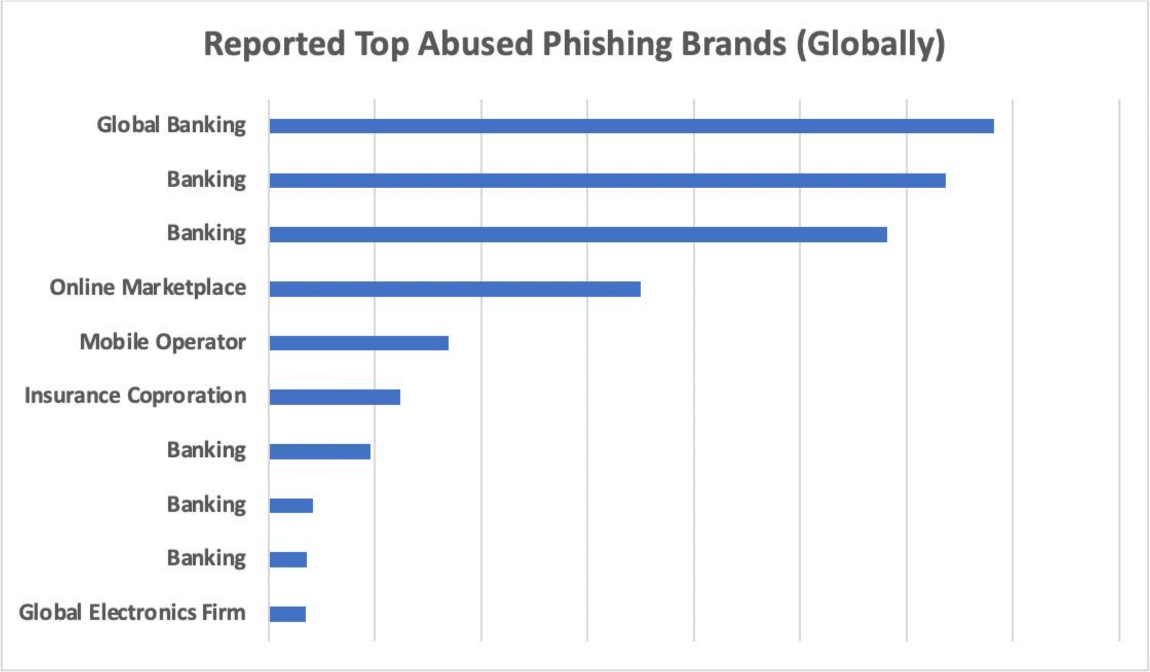


Figure 1 - Top Brands Featured in Mobile Messages, September 2020 [2]

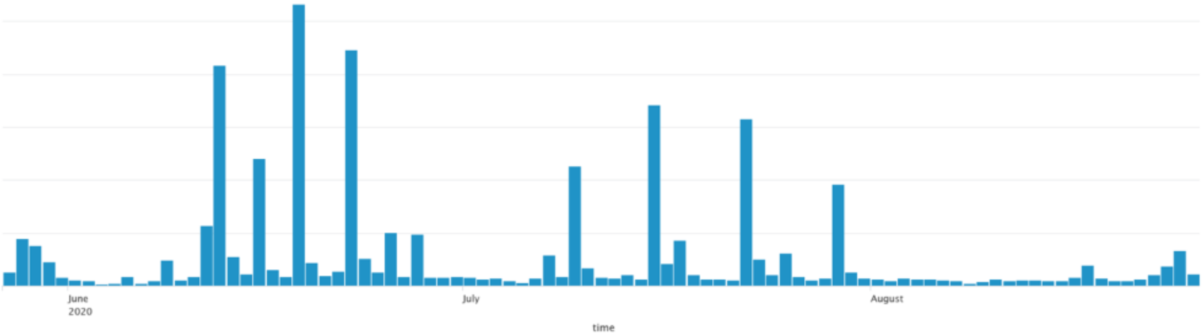
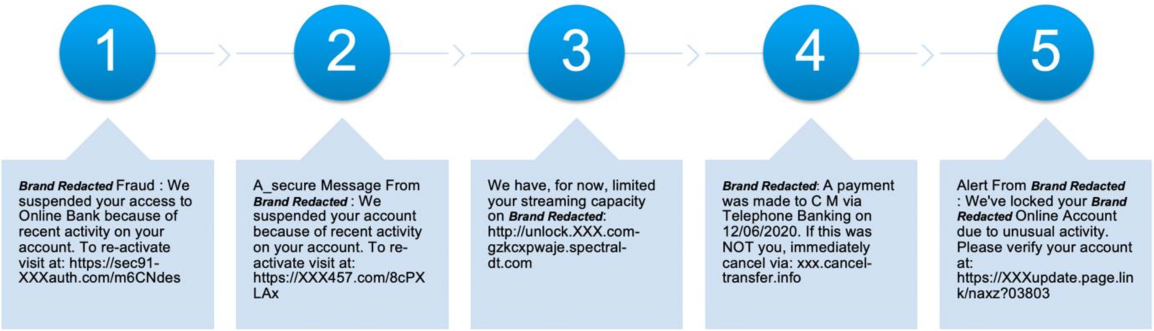


Figure 2 - June-August 2020 Mobile Phishing Report [2]


1

Brand Redacted Fraud : We suspended your access to Online Bank because of recent activity on your account. To re-activate visit at: https://sec91-XXXauth.com/m6CNdes

2

A_secure Message From ***Brand Redacted*** : We suspended your account because of recent activity on your account. To re-activate visit at: https://XXX457.com/8cPXLAx

3

We have, for now, limited your streaming capacity on ***Brand Redacted***: http://unlock.XXX.com-gzkcxpwaje.spectral-dt.com

4

Brand Redacted: A payment was made to C M via Telephone Banking on 12/06/2020. If this was NOT you, immediately cancel via: xxx.cancel-transfer.info

5

Alert From ***Brand Redacted*** : We've locked your ***Brand Redacted*** Online Account due to unusual activity. Please verify your account at: https://XXXupdate.page.link/naxz?03803

Figure 3 - Example SMS phishing messages using known brands [2]

Cybercriminals create and distribute mobile malware programmes, which are specifically designed to target a victim's mobile device. Premium-rate SMS scams include customers signing up for subscription message services without their permission. Victims receive unwelcome bills on their phone bills, and they may even be paying the attacker if these services are handled by the offender [3].

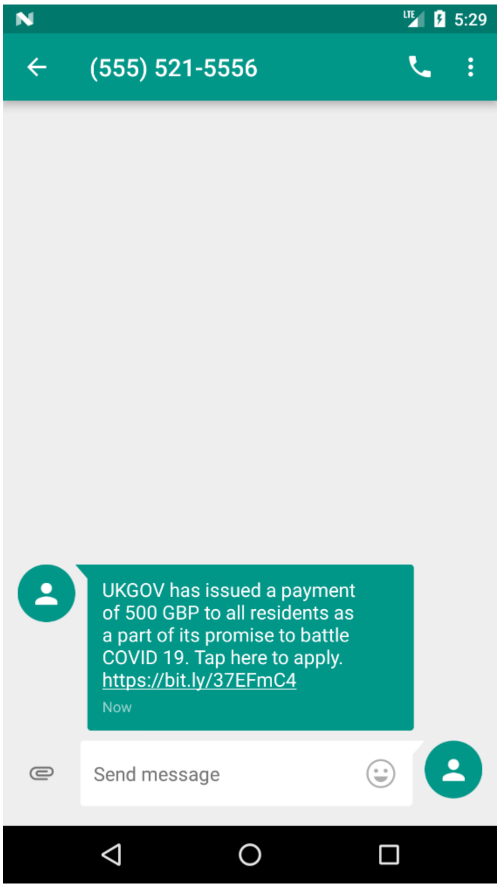
During the COVID 19 pandemic, the NHS, General Practitioners (GPs) and other government authorities used the SMS platform to spread awareness about the Coronavirus, lockdowns, and contact tracing and encouraged them to get vaccinated. As people were on fears of this predicament, they followed the text messages and clicked the links on these text messages to learn more about Covid and quarantine rules and regulations. This created fertile ground for scammers, and they began to seize the opportunity by making a wave of Covid pandemic-related hoax text messages that tricked the users into clicking on a harmful link.

[4] NextCaller estimates a 44% spike in scam phone calls and SMS messages, during the first two weeks of the worldwide quarantine period [5] (Figure 4).

COVID-19 HAS CAUSED AN INCREASE IN SMS-BASED ATTACKS
Hackers have sent out fake texts about:
BANK CHECK
How to receive stimulus checks
Where and how to get tested
And where and how to get a vaccine.

Figure 4 – Some covid 19 related scam messages [6]

Nowadays, there are a variety of text messages pretending to be from the Government, GP's surgery, the NHS, or even the World Health Organization (WHO). These scam texts frequently include untrustworthy links or attachments and push you to click on them (as illustrated on Figure 5. These links lead you to a phony website that requests personal, sensitive data [7].



UKGOV has issued a payment of 500 GBP to all residents as a part of its promise to battle COVID 19. Tap here to apply. https://bit.ly/37EFmC4

Now

Figure 5 – An example of a scam text message

In section 2, this paper aims to provide background information, an assessment of SMS system architecture, associated literature, and the scope and limitations of SMS attacks. Section 3 explains the methodology that uses the Dagah platform to demonstrate a real-world attack scenario and Wireshark for the identification and analysis of vulnerabilities. Section 4 describes the recommendations, and Section 5 draws the report to a conclusion.

2. BACKGROUND

Scam SMS is a term used to describe unwanted or unsolicited text messages sent to mobile phone users over the Short Messaging Service (SMS). It might be difficult for mobile users, particularly elderly users, to determine the legitimacy of a text message. One of the primary reasons SMS-based fraud is so successful is because of this.

SMS-based scams increased by 328% in the middle of 2020, according to Proofpoint. [2] (As shown in Figure 6)

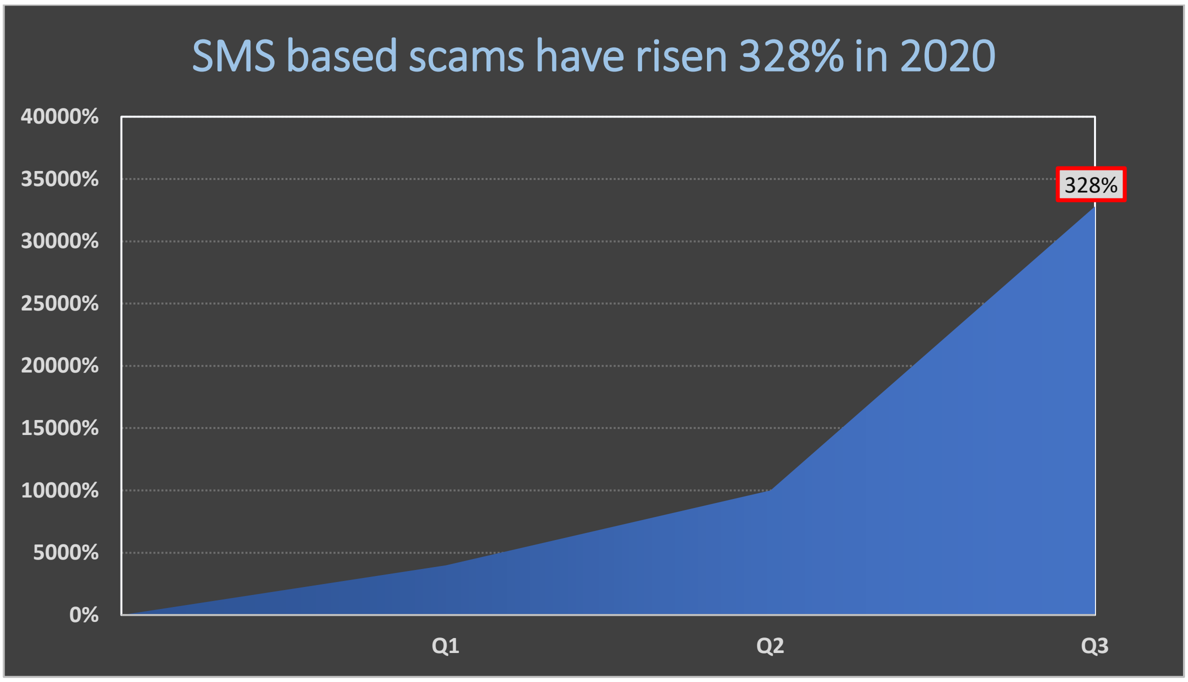


Figure 6 – SMS based scams have risen 328% in 2020 [2]

According to Proofpoint, a security software business that processes more than 80% of North America's mobile texts, only 23% of users over 55 were able to accurately identify smishing and millennials fared no better, with only 34% of persons 23-38 years old displaying awareness of the phrase as in Figure 7.

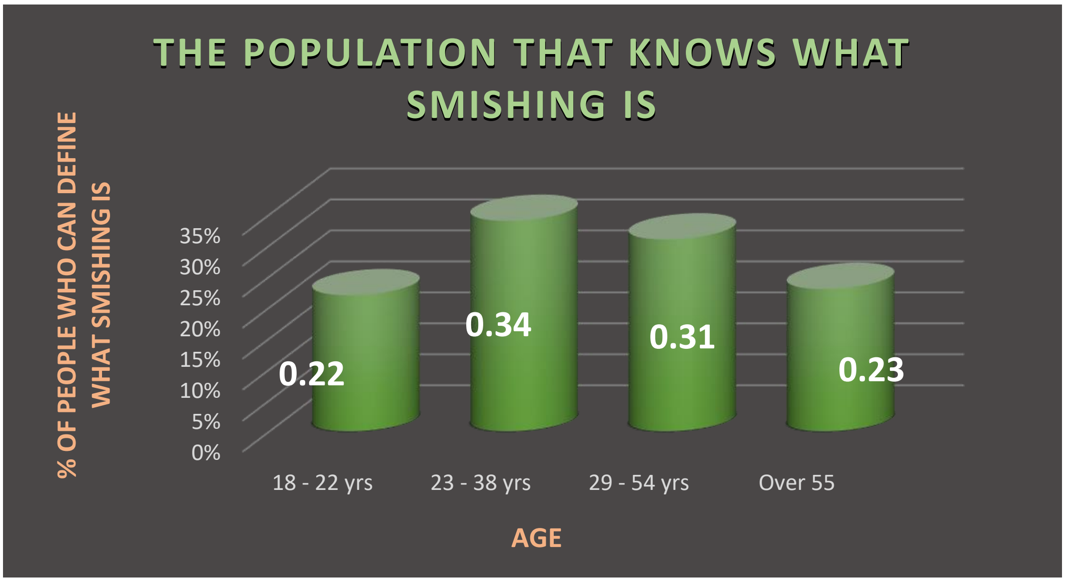


Figure 7 - The population that knows what smishing is [2]

The Bank of Ireland was compelled to pay out €800,000 to over 300 bank clients in a single smishing scam in 2020 [6]. Tax scams from Her Majesty's Revenue and Customs (HMRC) and Fake delivery notifications are the most common smishing attacks in the United Kingdom (Figure 8).

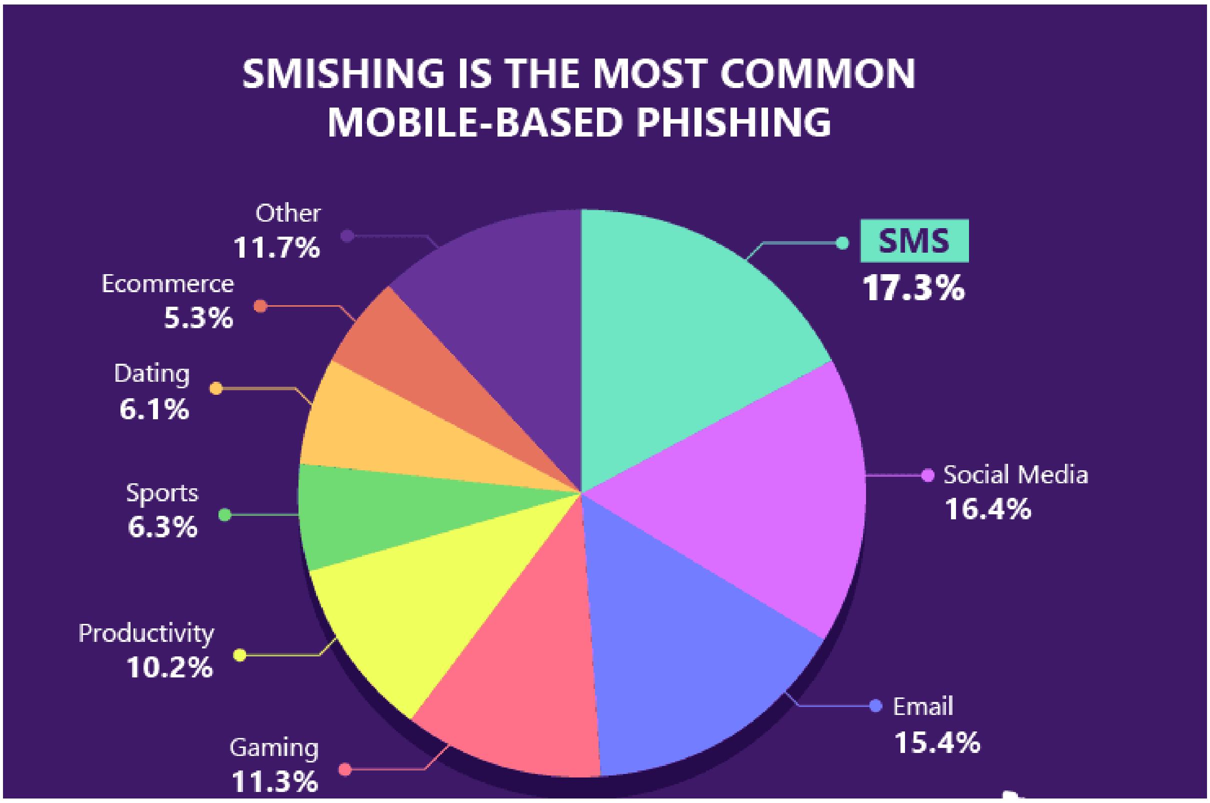


Figure 8 - Smishing is the most common type of mobile-based phishing [6]

Messages must go through three steps in order to be delivered: submission, routing, and transit medium as illustrated in Figure 9.

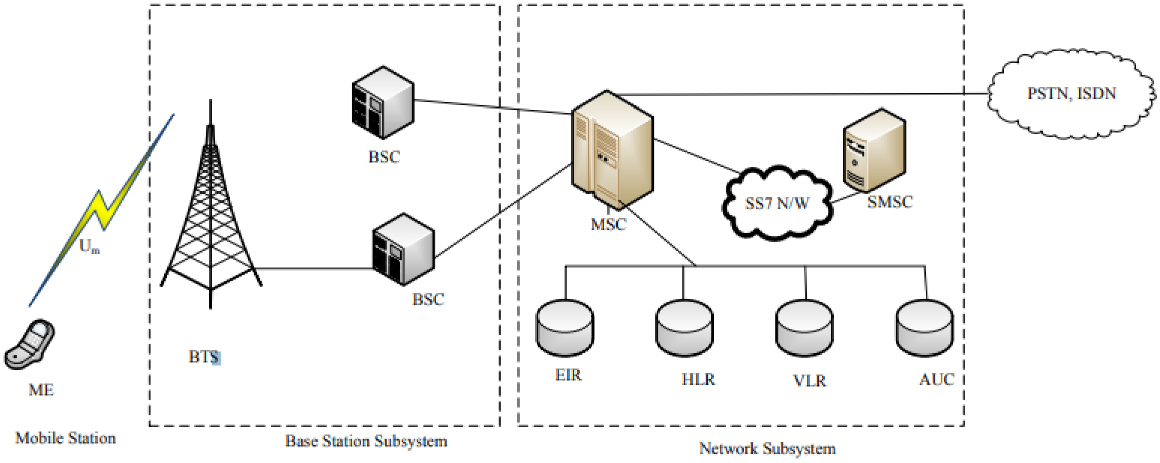


Figure 9 - GSM Network Architecture [8]

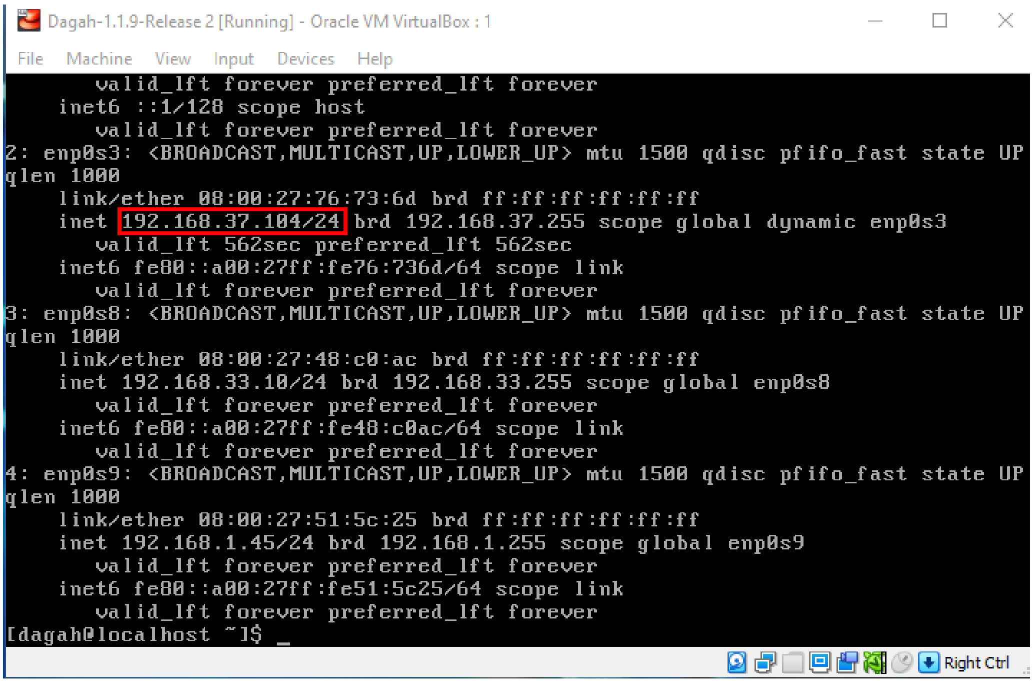
In the year 2020, a similar phone spear-phishing attempt was successfully undertaken on Twitter. As a result, some employees' credentials were compromised [9].

Spam SMS can be created using a variety of routes, including fake base stations [10], [11], [12] or SMS Gateways [13], [14], and is primarily connected with the illicit promotion or malware dissemination [15], [16], [17], [18] according to the previous research papers. Template-based clustering [19], [20], [16] topic analysis [21], and clustering based on the sending patterns of suspicious accounts [22] are the most common ways of detecting spam SMS. Despite the fact that various studies have been dedicated to identifying and evaluating the scam SMS ecology [21], [13], [14], [12] adversaries are continually developing, and new threats emerge in this field.

This research aims at the most devious social engineering threats such as, SMS-based smishing and mobile malware attacks. The scope of this document is to detect and defeat Advanced Persistent Threats (APT) and malicious programs from the perspective of Cyber Threat Intelligence (CTI). To effectively analyse malware, a proper testbed environment is required, which was not possible to set up in the current circumstances. Consequently, part of the malware analysis was performed on a limited scale, and another part from the literature is included, which was the main limitation of this research article.

3. METHODOLOGY

First, I set up Dagah Virtual Machine (VM) in VirtualBox (Figure 10) and accessed its web page using its IP address 192.168.37.104 as shown in Figure 11.



Dagah-1.1.9-Release 2 [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
Right Ctrl

```
        valid_lft forever preferred_lft forever
     inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
qlen 1000
     link/ether 08:00:27:76:73:6d brd ff:ff:ff:ff:ff:ff
     inet 192.168.37.104/24 brd 192.168.37.255 scope global dynamic enp0s3
        valid_lft 562sec preferred_lft 562sec
     inet6 fe80::a00:27ff:fe76:736d/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
qlen 1000
     link/ether 08:00:27:48:c0:ac brd ff:ff:ff:ff:ff:ff
     inet 192.168.33.10/24 brd 192.168.33.255 scope global enp0s8
        valid_lft forever preferred_lft forever
     inet6 fe80::a00:27ff:fe48:c0ac/64 scope link
        valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
qlen 1000
     link/ether 08:00:27:51:5c:25 brd ff:ff:ff:ff:ff:ff
     inet 192.168.1.45/24 brd 192.168.1.255 scope global enp0s9
        valid_lft forever preferred_lft forever
     inet6 fe80::a00:27ff:fe51:5c25/64 scope link
        valid_lft forever preferred_lft forever
[dagah@localhost ~]$ _
```

Figure 10 – Dagah account set up in VirtualBox

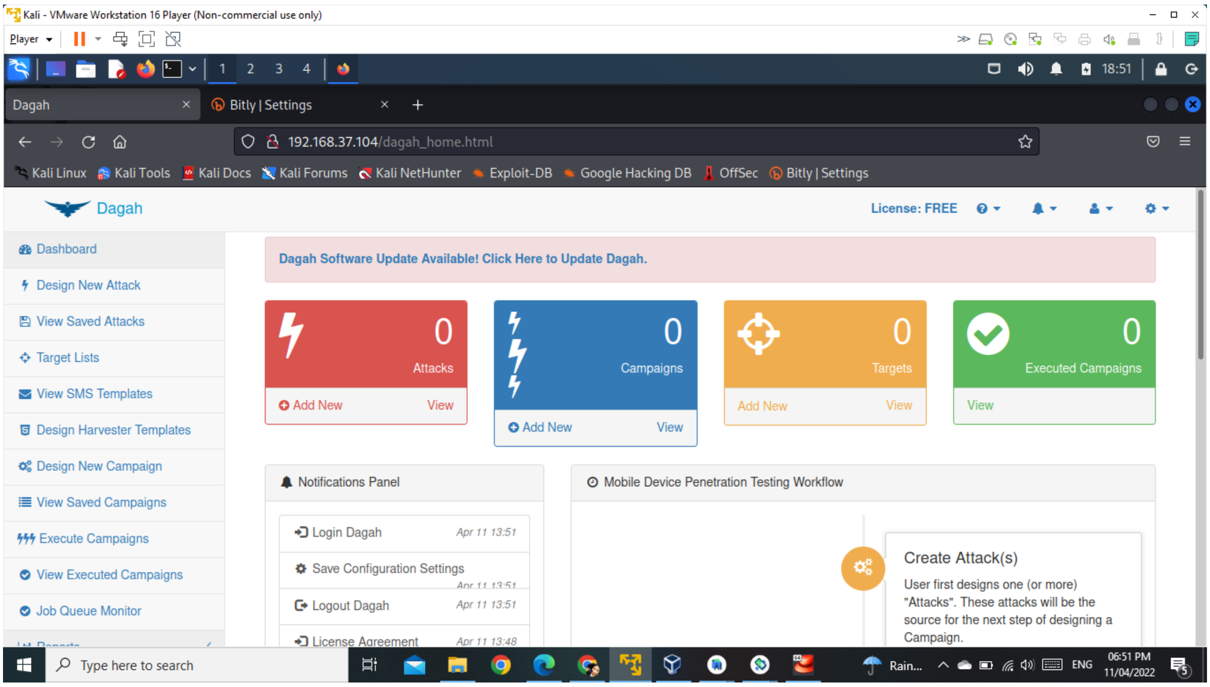
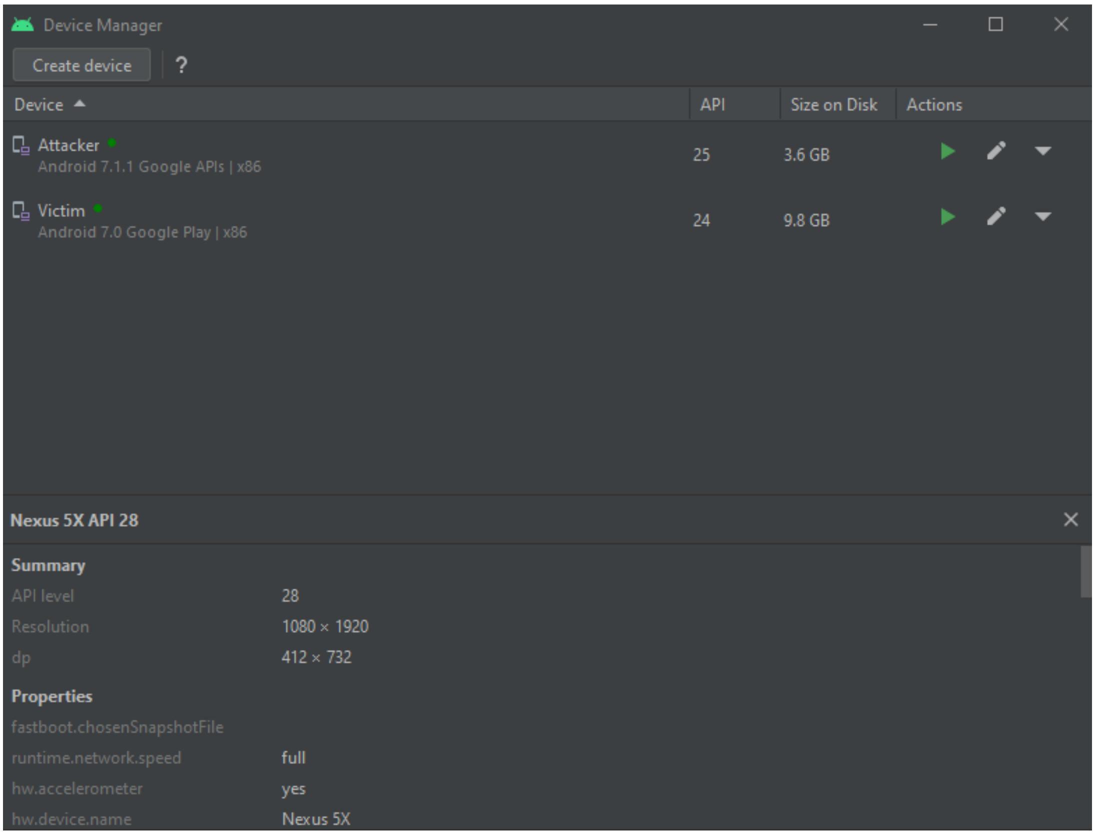


Figure 11 – Dagah Web page using the IP address 192.168.37.104

Then I installed Android Studio and created two virtual mobile phones that run Android versions 7.1.1 and 7.0 using Android Virtual Device (AVD) Manager as shown in Figure 12.



Device	API	Size on Disk	Actions
Attacker Android 7.1.1 Google APIs | x86	25	3.6 GB	
Victim Android 7.0 Google Play | x86	24	9.8 GB	

Nexus 5X API 28

Summary

API level	28
Resolution	1080 × 1920
dp	412 × 732

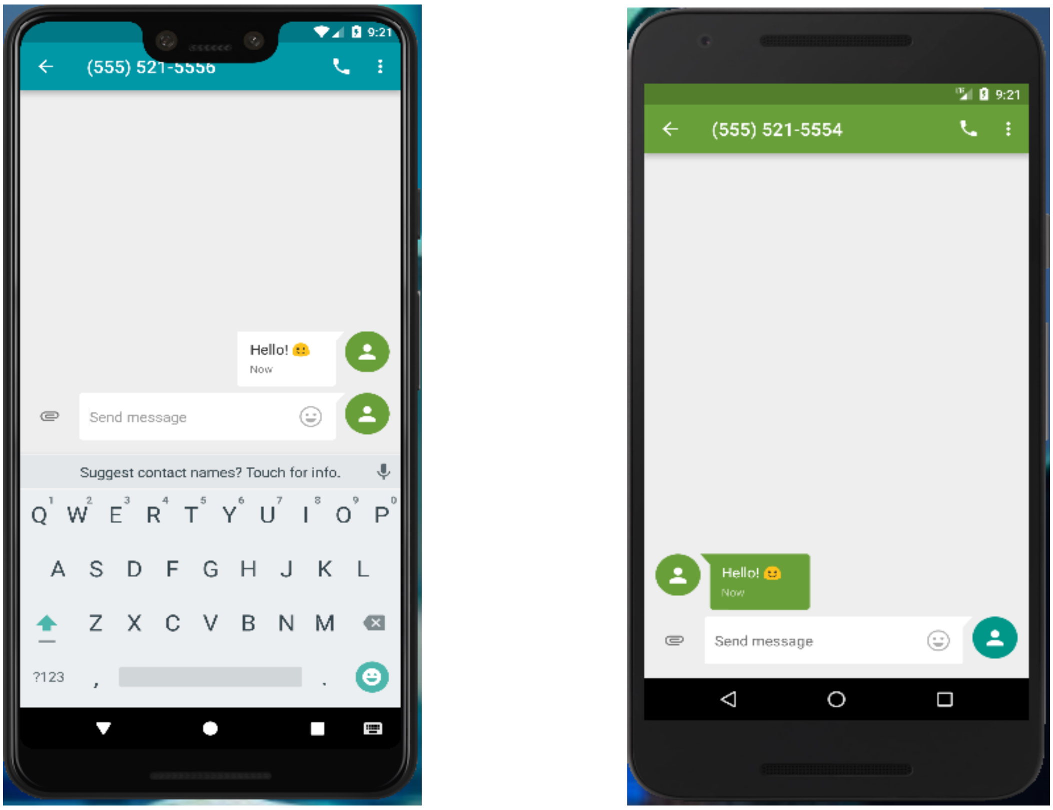
Properties

fastboot.chosenSnapshotFile	
runtime.network.speed	full
hw.accelerometer	yes
hw.device.name	Nexus 5X

Figure 12 – Virtual mobile phones created using AVD Manager

As shown in Figure 13, we can send text messages from one mobile phone to another, implying that they can communicate with one other. One mobile phone acted as the attacker and its phone number is +1-555-521-5554, whereas the other phone acted as the victim and its phone number is +1-555-521-5556. I also tested the Internet connectivity of both phones and confirmed that they were both connected (as in Figure 14).

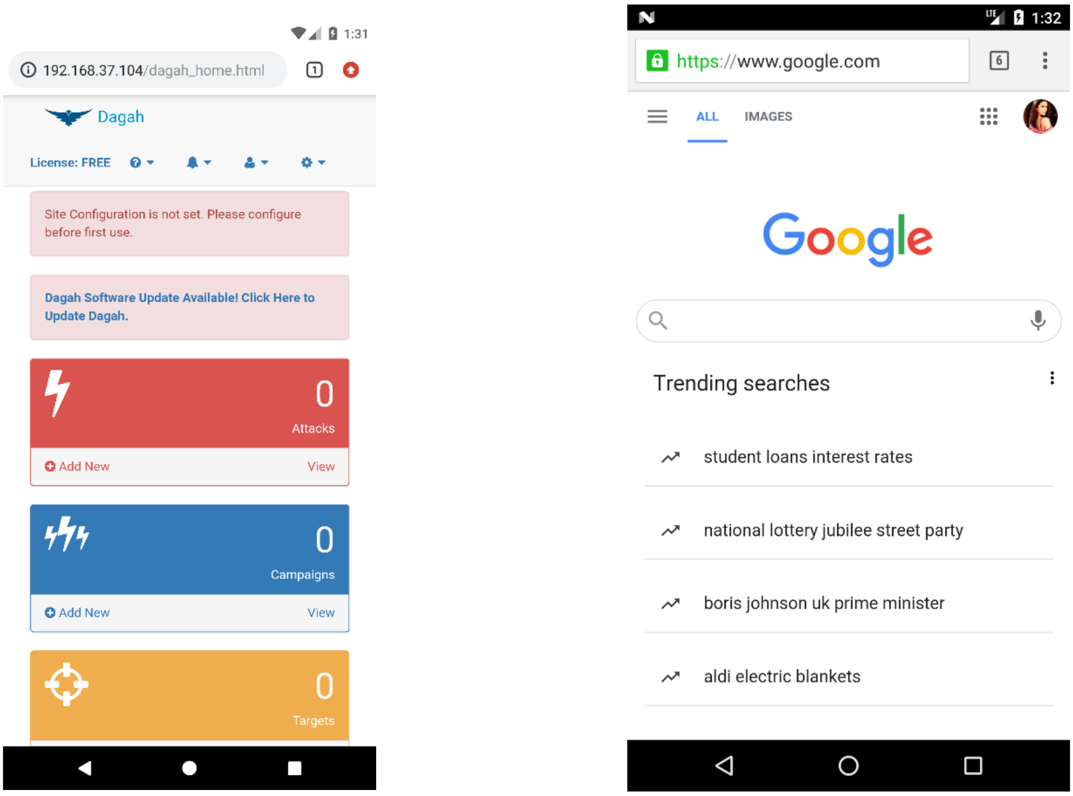
Afterward, I created a bitly account on bitly.com to receive an access token for shortening URLs (Figure 15) and to manage the links associated with the SMS attack on the simulated smartphone I created earlier. I entered the attacker's phone number, generated bitly Token, IP address, Shell IP address, Modem type, Modem Number etc into the Dagah website for configuration (refer Figures 16a, 16b, 16c, and 16d). As illustrated in Figure 17, I accessed the Dagah web page from the attacker's phone and signed into my account and downloaded the Dagah Modem Bridge application and installed it. The attacker’s phone is now prepared for the attack.



Hello!
Now

Hello!
Now

Figure 13 – Sending text messages to check the communication between two mobile devices



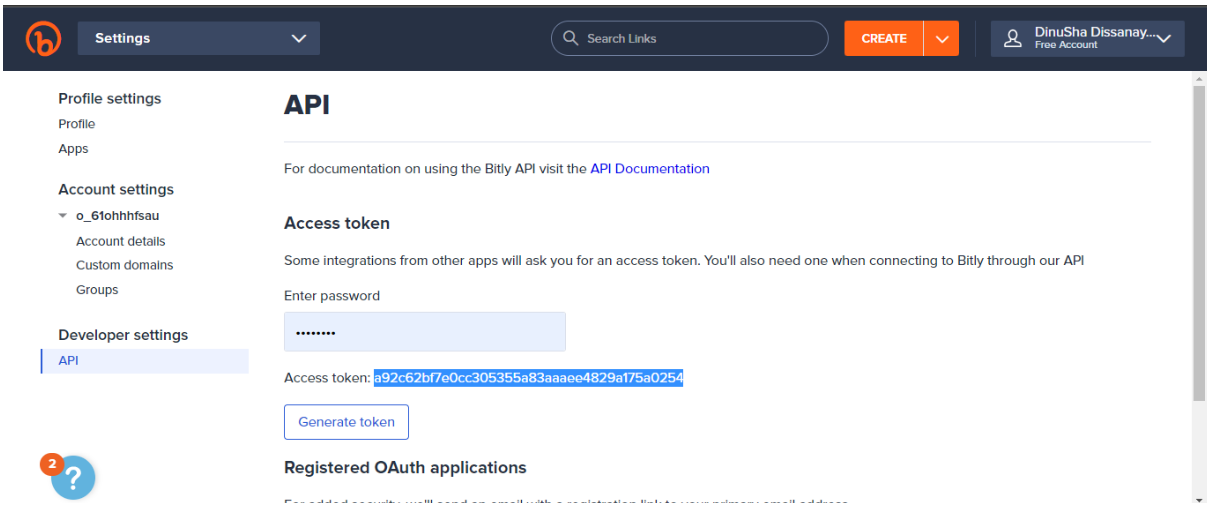
Site Configuration is not set. Please configure before first use.

Dagah Software Update Available! Click Here to Update Dagah.

Trending searches

- student loans interest rates
- national lottery jubilee street party
- boris johnson uk prime minister
- aldi electric blankets

Figure 14 – Checking internet connectivity of both mobile devices



API

For documentation on using the Bitly API visit the API Documentation

Access token

Some integrations from other apps will ask you for an access token. You'll also need one when connecting to Bitly through our API

Enter password

••••••••

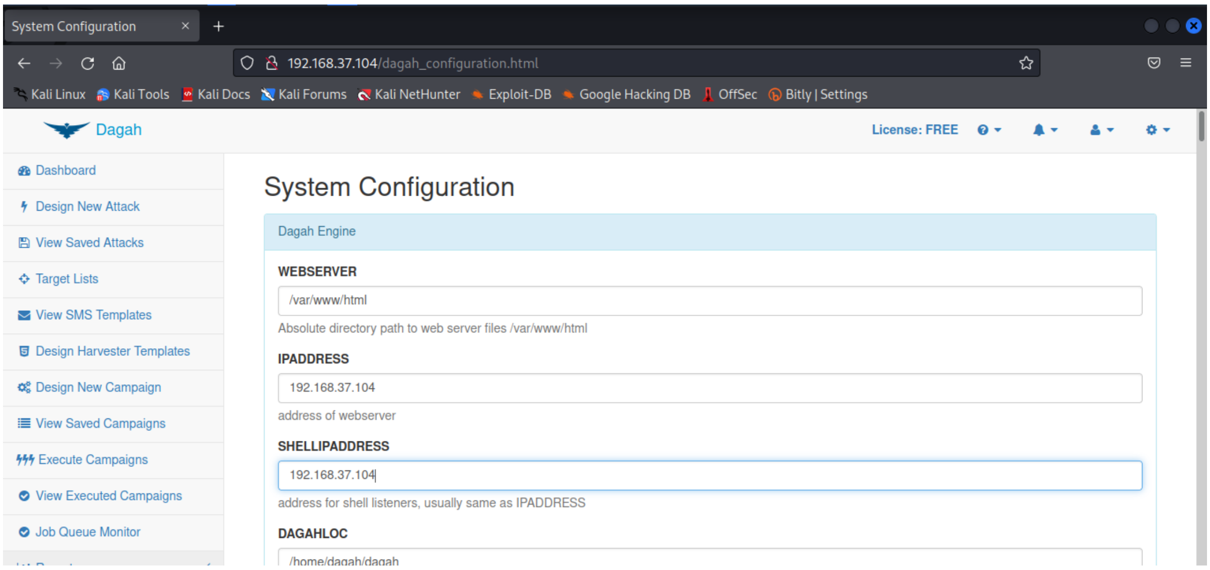
Access token: a92c62bf7e0cc305355a83aaaee4829a175a0254

Generate token

Registered OAuth applications

For added security, we'll send an email with a registration link to your primary email address

Figure 15 – Access token generated in Bitly account



System Configuration

Dagah Engine

WEBSERVER

/var/www/html

Absolute directory path to web server files /var/www/html

IPADDRESS

192.168.37.104

address of webserver

SHELLIPADDRESS

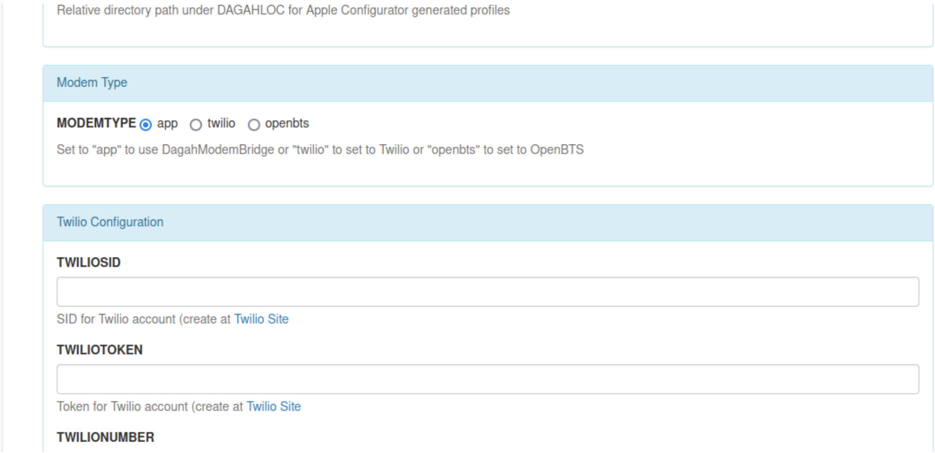
192.168.37.104

address for shell listeners, usually same as IPADDRESS

DAGAHLOC

/home/dagah/dagah

Figure 16a - Dagah website configuration



Relative directory path under DAGAHLOC for Apple Configurator generated profiles

Modem Type

MODEMTYPE ● app ○ twilio ○ openbts

Set to "app" to use DagahModemBridge or "twilio" to set to Twilio or "openbts" to set to OpenBTS

Twilio Configuration

TWILIOSID

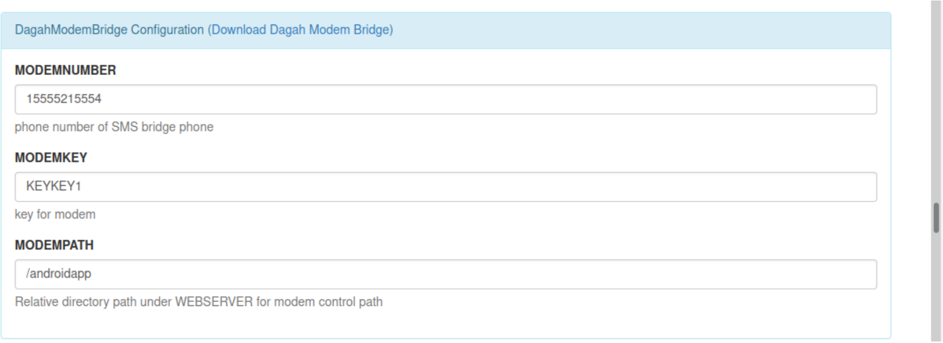
SID for Twilio account (create at Twilio Site

TWILIOTOKEN

Token for Twilio account (create at Twilio Site

TWILIONUMBER

Figure 16b – Dagah website configuration



DagahModemBridge Configuration (Download Dagah Modem Bridge)

MODEMNUMBER

15555215554

phone number of SMS bridge phone

MODEMKEY

KEYKEY1

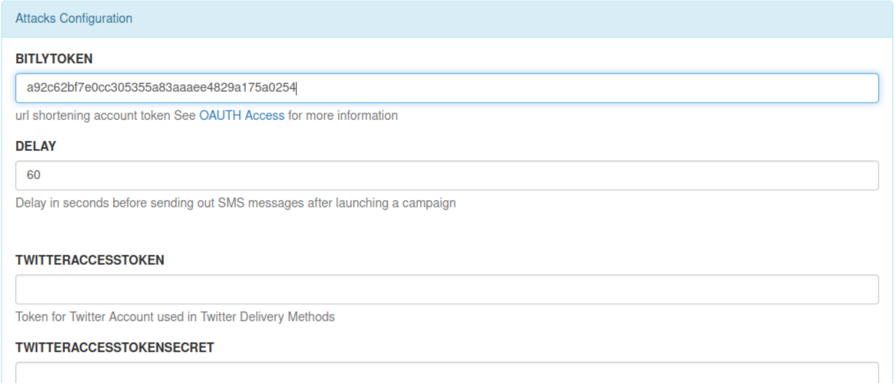
key for modem

MODEMPATH

/androidapp

Relative directory path under WEBSERVER for modem control path

Figure 16c - Dagah website configuration



Attacks Configuration

BITLYTOKEN

a92c62bf7e0cc305355a83aaaee4829a175a0254

url shortening account token See OAUTH Access for more information

DELAY

60

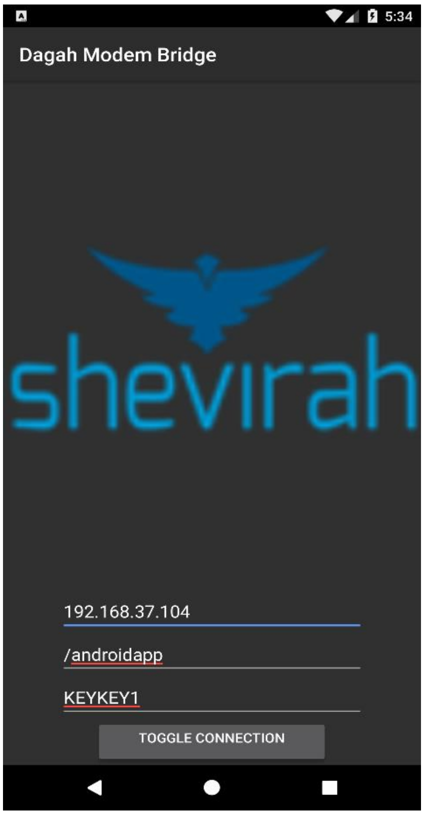
Delay in seconds before sending out SMS messages after launching a campaign

TWITTERACCESSTOKEN

Token for Twitter Account used in Twitter Delivery Methods

TWITTERACCESSTOKENSECRET

Figure 16d - Dagah website configuration with the generated access token



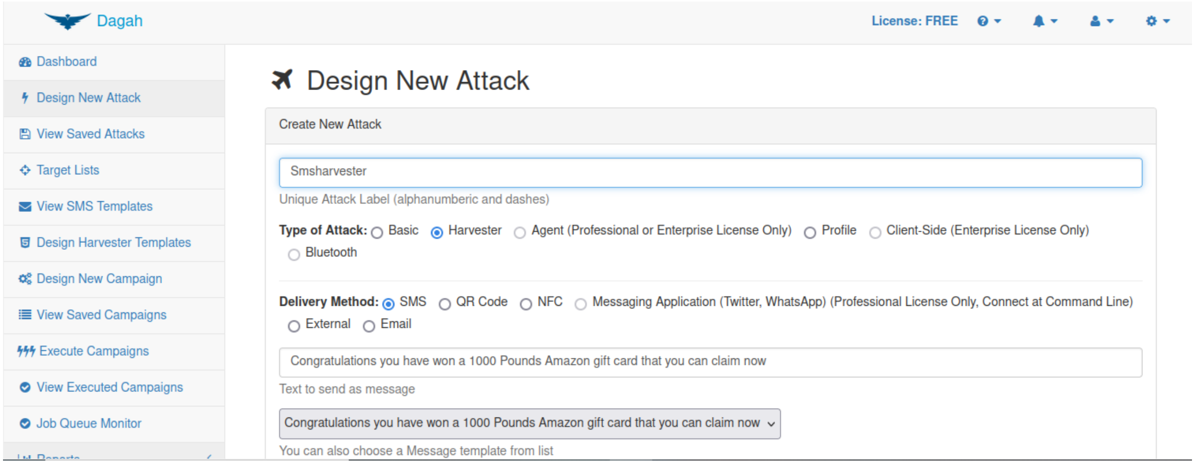
192.168.37.104

/androidapp

KEYKEY1

Figure 17– Dagah Modem Bridge application

I created an SMS-based Social Engineering attack against the Dagah website, as shown in Figures 18a, 18b, 18c, and 18d. The goal of the attack was to get access to the victim's Gmail account credentials. The target was identified by giving Dagah the victim's phone number, and the attack was carried out, as shown in Figure 18e. When the attack was carried out, the victim's mobile phone received an SMS message from the attacker's phone number, as shown in Figure 19. The SMS message was designed using Social Engineering techniques to trick the victim into entering his Gmail credentials into a fake Gmail login page that looks exactly like the original Gmail login web page. The user was routed to a phony Gmail Login page after clicking the malicious link supplied in the SMS. We can observe in Figure 20 that the victim is inputting his credentials. When the victim inputs his username and password, Dagah records these and shows them in plain text in the Campaign Results section of its website, as shown in Figure 21. As a result, the victim's Gmail account credentials were compromised utilising an SMS-based Social Engineering attack in this attack.



Design New Attack

Create New Attack

Smsharvester

Unique Attack Label (alphanumberic and dashes)

Type of Attack: ○ Basic ● Harvester ○ Agent (Professional or Enterprise License Only) ○ Profile ○ Client-Side (Enterprise License Only) ○ Bluetooth

Delivery Method: ● SMS ○ QR Code ○ NFC ○ Messaging Application (Twitter, WhatsApp) (Professional License Only, Connect at Command Line) ○ External ○ Email

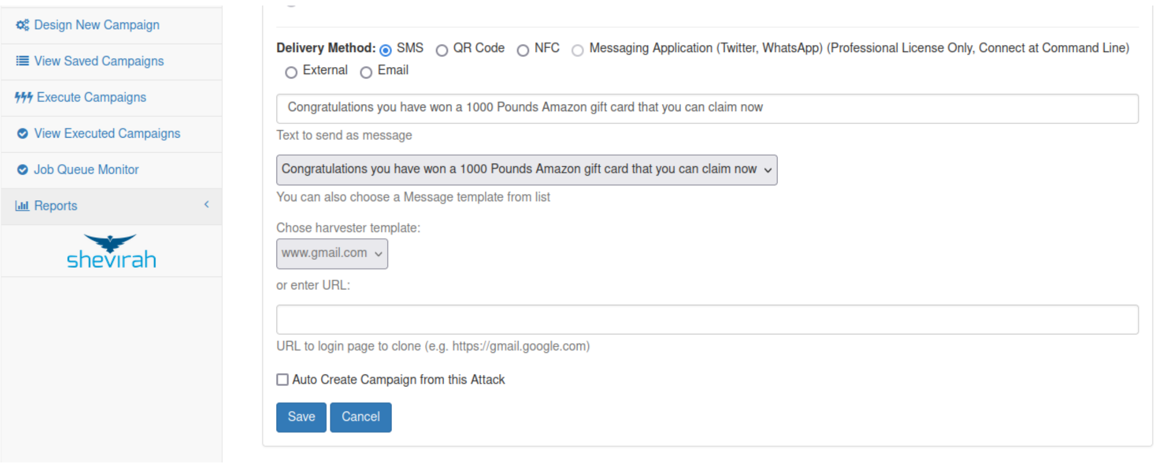
Congratulations you have won a 1000 Pounds Amazon gift card that you can claim now

Text to send as message

Congratulations you have won a 1000 Pounds Amazon gift card that you can claim now

You can also choose a Message template from list

Figure 18a – Creating a new SMS Harvester attack



Delivery Method: ● SMS ○ QR Code ○ NFC ○ Messaging Application (Twitter, WhatsApp) (Professional License Only, Connect at Command Line) ○ External ○ Email

Congratulations you have won a 1000 Pounds Amazon gift card that you can claim now

Text to send as message

Congratulations you have won a 1000 Pounds Amazon gift card that you can claim now

You can also choose a Message template from list

Chose harvester template:

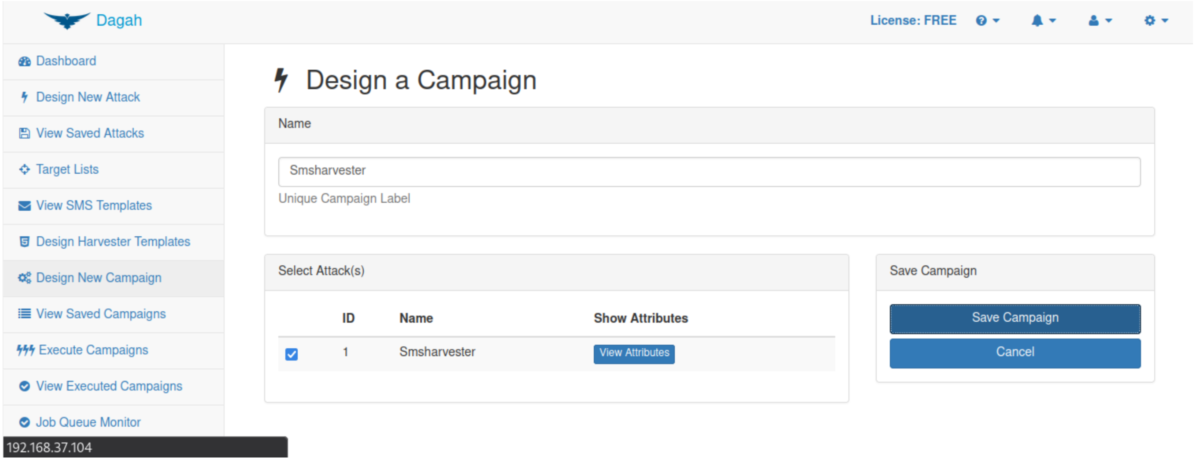
www.gmail.com

or enter URL:

URL to login page to clone (e.g. https://gmail.google.com)

□ Auto Create Campaign from this Attack

Figure 18b – SMS Harvester attack with a fake Gmail login



Design a Campaign

Name

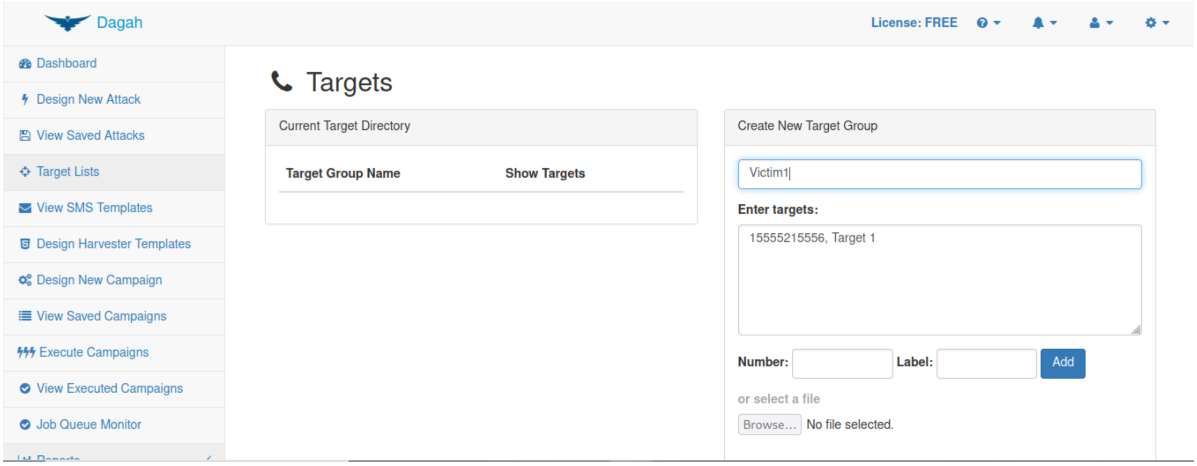
Smsharvester

Unique Campaign Label

Select Attack(s)

	ID	Name	Show Attributes
☑	1	Smsharvester	View Attributes

Figure 18c - Creating a campaign for the new attack



Targets

Current Target Directory

Target Group Name	Show Targets

Create New Target Group

Victim1

Enter targets:

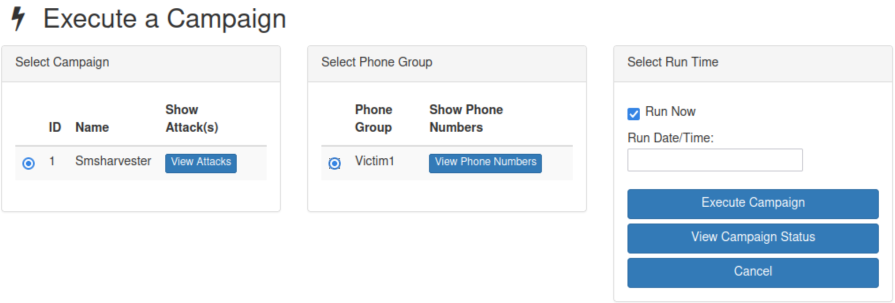
15555215556, Target 1

Number: Label:

or select a file

No file selected.

Figure 18d – Creating a target group for the attack



Execute a Campaign

Select Campaign

	ID	Name	Show Attack(s)
◉	1	Smsharvester	View Attacks

Select Phone Group

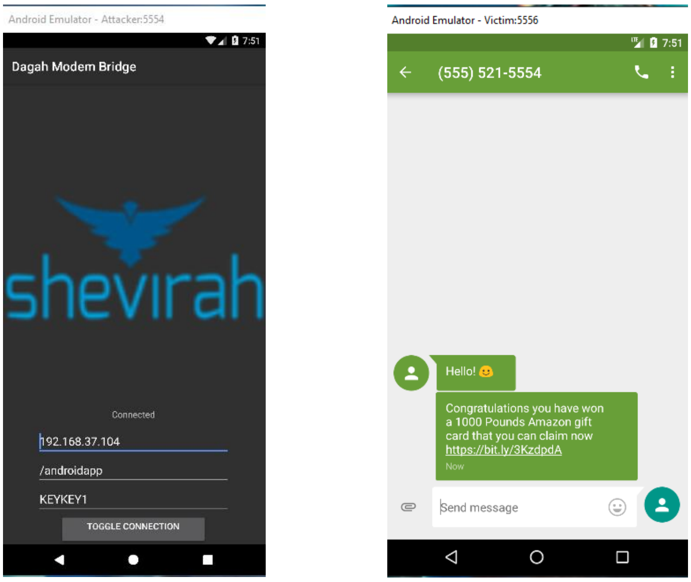
	Phone Group	Show Phone Numbers
◉	Victim1	View Phone Numbers

Select Run Time

☑ Run Now

Run Date/Time:

Figure 18e – Executed the attack



Connected

192.168.37.104

/androidapp

KEYKEY1

Hello! 😃

Congratulations you have won a 1000 Pounds Amazon gift card that you can claim now https://bit.ly/3KzdpdA

Now

Figure 19 – The attacker’s phone connected to the Dagah server using the installed software, and the victim’s phone received the executed scam text message.

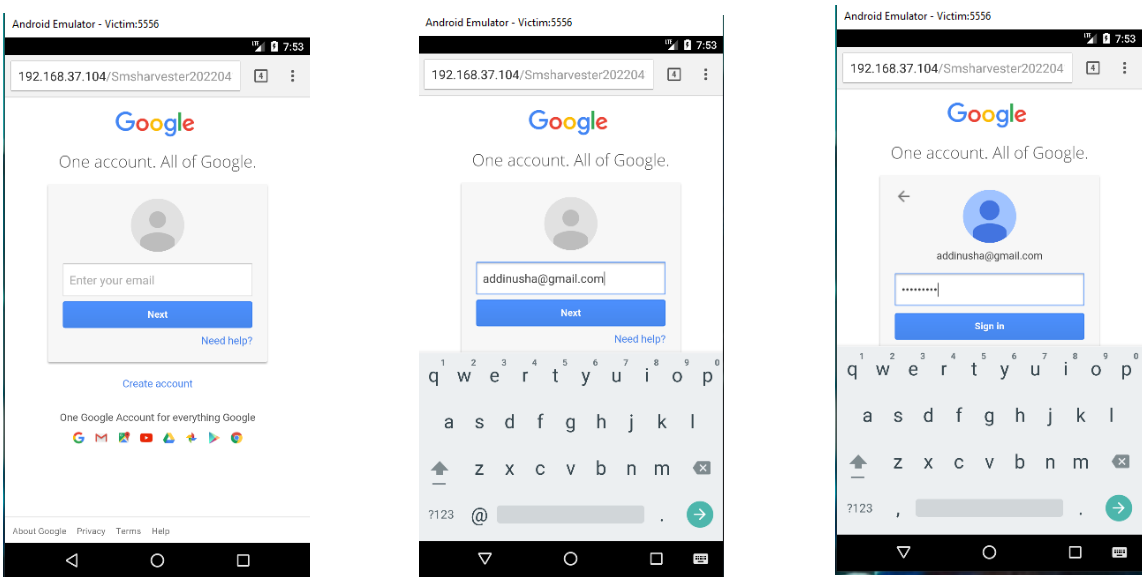
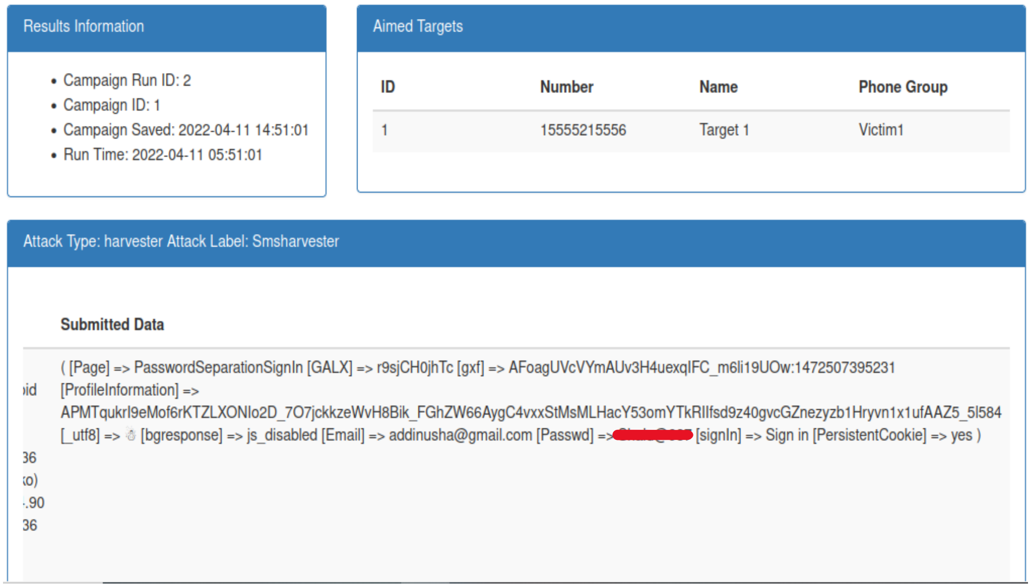


Figure 20 – The fake Gmail login page once the victim clicks the link on the SMS



Results Information

- Campaign Run ID: 2
- Campaign ID: 1
- Campaign Saved: 2022-04-11 14:51:01
- Run Time: 2022-04-11 05:51:01

Aimed Targets

ID	Number	Name	Phone Group
1	15555215556	Target 1	Victim1

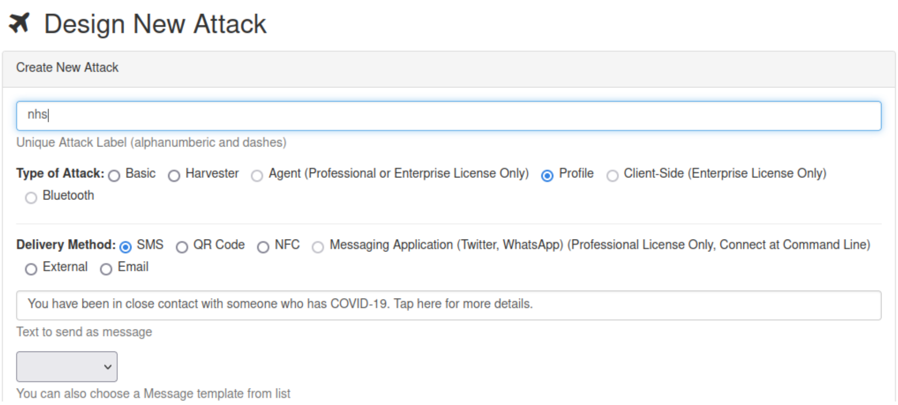
Attack Type: harvester Attack Label: Smsharvester

Submitted Data

```
    ( [Page] => PasswordSeparationSignIn [GALX] => r9sjCH0jhTc [gxf] => AFoagUVcVYmAUv3H4uexqIFC_m6li19UOw:1472507395231
id  [ProfileInformation] =>
    APMTqukrI9eMof6rKTZLXONIo2D_7O7jckkzeWvH8Bik_FGhZW66AygC4vxxStMsMLHacY53omYTkRIlfsd9z40gvcGZnezyzb1Hryvn1x1ufAAZ5_5l584
    [_utf8] => ☃ [bgresponse] => js_disabled [Email] => addinusha@gmail.com [Passwd] =>[redacted] [signIn] => Sign in [PersistentCookie] => yes )
36
o)
.90
36
```

Figure 21 – Login credentials of the victim captured by Dagah.

Another social engineering attack was created to install malicious software on a victim's phone. First, created a new attack in Dagah by selecting the Profile as the attack type (Figure 22a). With this form of attack, a malicious file can be uploaded and linked to the URL specified in the SMS. Then uploaded the Virus.apk file as illustrated in Figure 22b. The attack was then carried out as earlier from the Dagah site (Figures 22c and 22d), and the victim received an SMS from the attacker's phone, as shown in Figure 23. When the victim clicked the link, he was prompted to download the Virus.apk file that the attacker had attached to the link, which was then downloaded onto the victim's phone, as shown in Figure 24. The victim's phone was compromised after the installation.



Design New Attack

Create New Attack

nhs

Unique Attack Label (alphanumberic and dashes)

Type of Attack: ○ Basic ○ Harvester ○ Agent (Professional or Enterprise License Only) ● Profile ○ Client-Side (Enterprise License Only) ○ Bluetooth

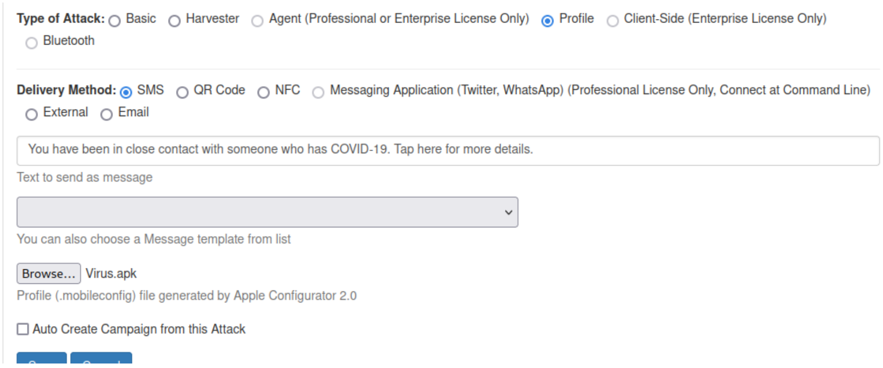
Delivery Method: ● SMS ○ QR Code ○ NFC ○ Messaging Application (Twitter, WhatsApp) (Professional License Only, Connect at Command Line) ○ External ○ Email

You have been in close contact with someone who has COVID-19. Tap here for more details.

Text to send as message

You can also choose a Message template from list

Figure 22a – Creating a SMS Profile attack with a Covid 19 related scam message



Type of Attack: ○ Basic ○ Harvester ○ Agent (Professional or Enterprise License Only) ● Profile ○ Client-Side (Enterprise License Only) ○ Bluetooth

Delivery Method: ● SMS ○ QR Code ○ NFC ○ Messaging Application (Twitter, WhatsApp) (Professional License Only, Connect at Command Line) ○ External ○ Email

You have been in close contact with someone who has COVID-19. Tap here for more details.

Text to send as message

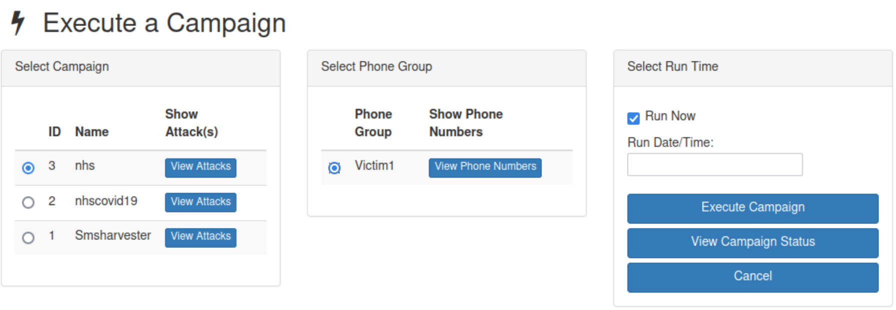
You can also choose a Message template from list

Browse... Virus.apk

Profile (.mobileconfig) file generated by Apple Configurator 2.0

☐ Auto Create Campaign from this Attack

Figure 22b – Attaching a malware apk file to the attack



Execute a Campaign

Select Campaign

	ID	Name	Show Attack(s)
●	3	nhs	View Attacks
○	2	nhscovid19	View Attacks
○	1	Smsharvester	View Attacks

Select Phone Group

	Phone Group	Show Phone Numbers
●	Victim1	View Phone Numbers

Select Run Time

☑ Run Now

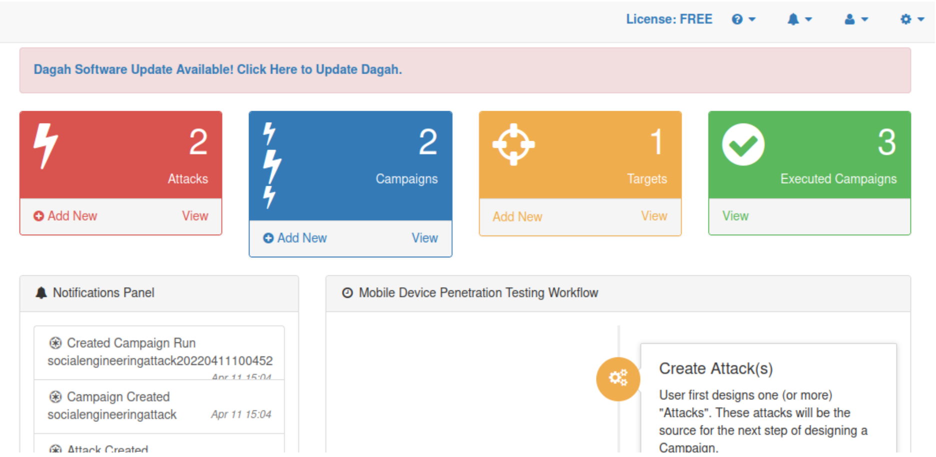
Run Date/Time:

Execute Campaign

View Campaign Status

Cancel

Figure 22c – Executing SMS profile attack



License: FREE

Dagah Software Update Available! Click Here to Update Dagah.

Notifications Panel

Created Campaign Run socialengineeringattack20220411100452 Apr 11 15:04

Campaign Created socialengineeringattack Apr 11 15:04

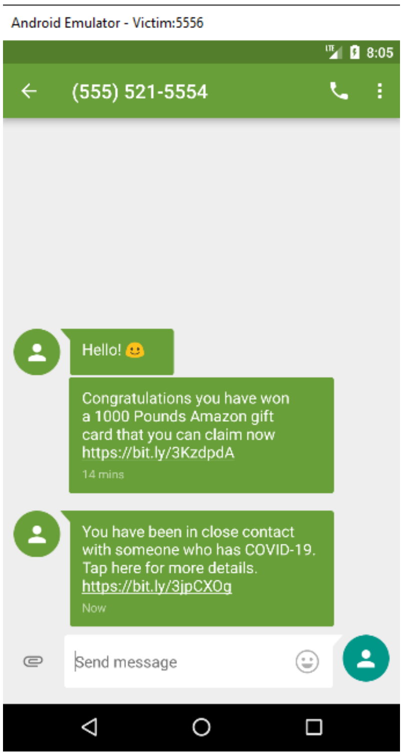
Attack Created

Mobile Device Penetration Testing Workflow

Create Attack(s)

User first designs one (or more) "Attacks". These attacks will be the source for the next step of designing a Campaign.

Figure 22d – Dagah dashboard summary



Android Emulator - Victim:5556

Hello! 😃

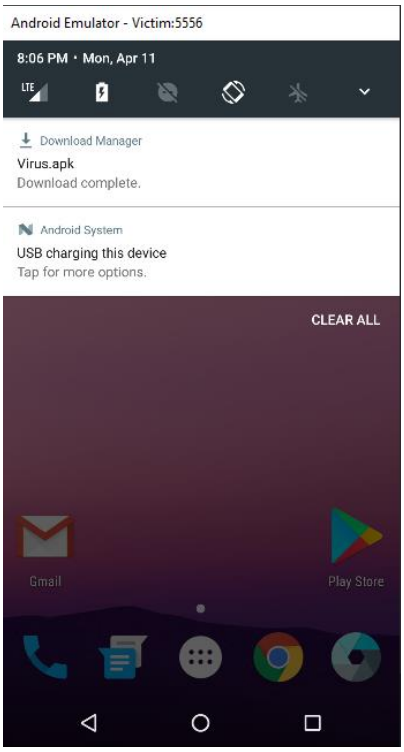
Congratulations you have won a 1000 Pounds Amazon gift card that you can claim now https://bit.ly/3KzdpdA

14 mins

You have been in close contact with someone who has COVID-19. Tap here for more details. https://bit.ly/3jpCXOg

Now

Figure 23– SMS scam message that contains the malware apk file



Android Emulator - Victim:5556

8:06 PM • Mon, Apr 11

Download Manager
Virus.apk
Download complete.

Android System
USB charging this device
Tap for more options.

Figure 24 – Virus.apk file that downloaded into Victim’s mobile device

4. ANALYSIS

Vulnerability Identification

Many people believe that their smartphones are safer than their computers. But smartphone security is limited, and it cannot defend against SMS-based attacks directly. Cybercrime directed at mobile devices is on the rise, as is mobile device usage.

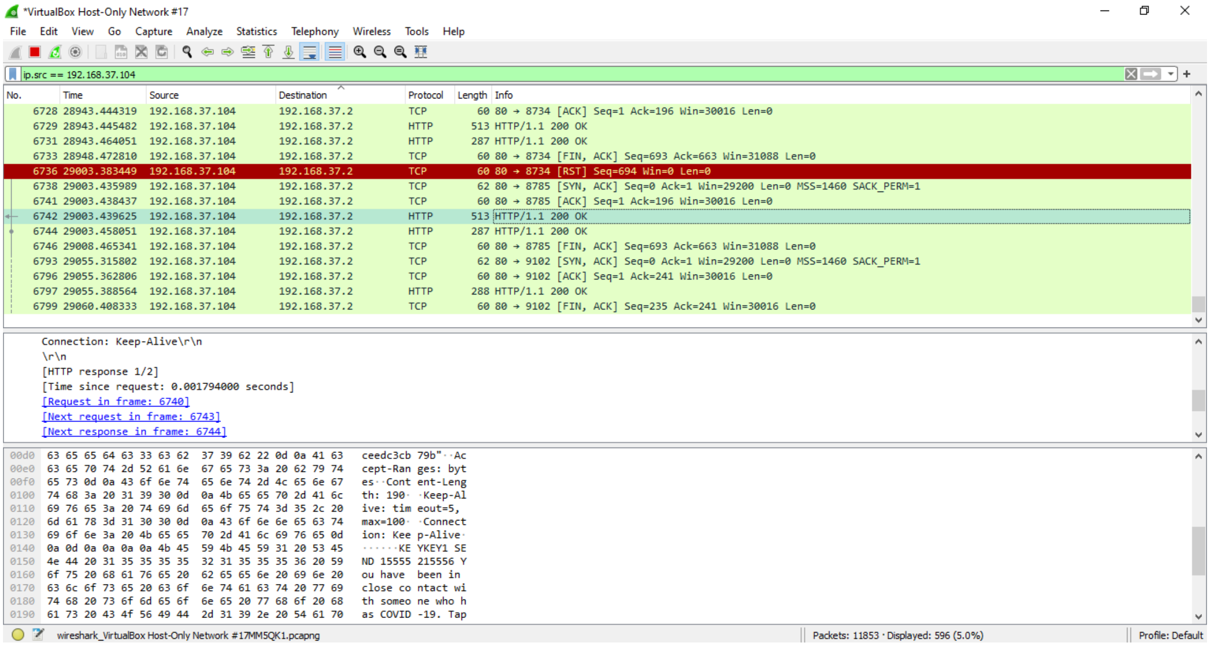
While Android smartphones remain the most popular target for malware because there are so many of them, and the platform provides more freedom for customers (and cybercriminals), smishing, like SMS-based cross-platform. Because iPhone and iPad users typically believe they are immune to attack, they are also equally vulnerable. Despite the fact that Apple's iOS mobile technology has a high-security reputation, no mobile operating system can defend you from phishing-style attacks on its own.

Another danger factor is that you use your smartphone while on the go, frequently when distracted or in a hurry. When you receive a message asking for bank information or to redeem a coupon, you're more likely to let your guard down and answer without thinking [23].

Network Analysis

When the attack is carried out, we will need to monitor the network traffic generated in the process of the attack; this will allow us to detect the communication channel and network-based indicators of the attack.

The network traffic was monitored using Wireshark on the Dagah server after an attack was launched. The traffic captured by Wireshark is seen in the following screenshot (Figure 25a & 25b). The victim's mobile device (192.168.37.2) is attempting to communicate with the C2 server by resolving the C2 domain, which is resolved to the Dagah server IP address of 192.168.37.104. Once resolved, it then makes an HTTP communication to download the Virus.apk file


*VirtualBox Host-Only Network #17
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.src == 192.168.37.104
```

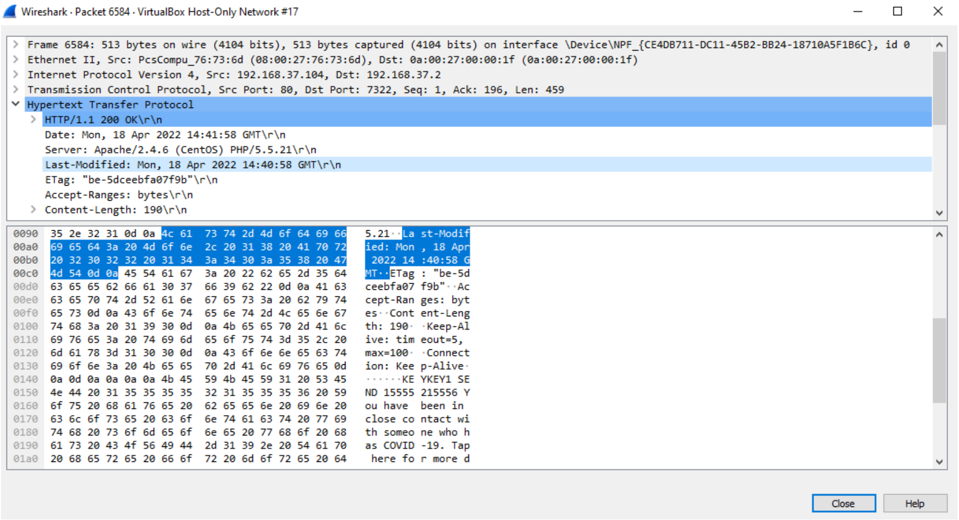
```
No.   Time            Source          Destination    Protocol Length Info
 6728 28943.444319    192.168.37.104  192.168.37.2   TCP        60 80 → 8734 [ACK] Seq=1 Ack=196 Win=30016 Len=0
 6729 28943.445482    192.168.37.104  192.168.37.2   HTTP      513 HTTP/1.1 200 OK
 6731 28943.464051    192.168.37.104  192.168.37.2   HTTP      287 HTTP/1.1 200 OK
 6733 28948.472810    192.168.37.104  192.168.37.2   TCP        60 80 → 8734 [FIN, ACK] Seq=693 Ack=663 Win=31088 Len=0
 6736 29003.383449    192.168.37.104  192.168.37.2   TCP        60 80 → 8734 [RST] Seq=694 Win=0 Len=0
 6738 29003.435989    192.168.37.104  192.168.37.2   TCP        62 80 → 8785 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1
 6741 29003.438437    192.168.37.104  192.168.37.2   TCP        60 80 → 8785 [ACK] Seq=1 Ack=196 Win=30016 Len=0
 6742 29003.439625    192.168.37.104  192.168.37.2   HTTP      513 HTTP/1.1 200 OK
 6744 29003.458051    192.168.37.104  192.168.37.2   HTTP      287 HTTP/1.1 200 OK
 6746 29008.465341    192.168.37.104  192.168.37.2   TCP        60 80 → 8785 [FIN, ACK] Seq=693 Ack=663 Win=31088 Len=0
 6793 29055.315802    192.168.37.104  192.168.37.2   TCP        62 80 → 9102 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1
 6796 29055.362806    192.168.37.104  192.168.37.2   TCP        60 80 → 9102 [ACK] Seq=1 Ack=241 Win=30016 Len=0
 6797 29055.388564    192.168.37.104  192.168.37.2   HTTP      288 HTTP/1.1 200 OK
 6799 29060.408333    192.168.37.104  192.168.37.2   TCP        60 80 → 9102 [FIN, ACK] Seq=235 Ack=241 Win=30016 Len=0
```

```
    Connection: Keep-Alive\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.001794000 seconds]
    [Request in frame: 6740]
    [Next request in frame: 6743]
    [Next response in frame: 6744]
```

```
00d0  63 65 65 64 63 33 63 62  37 39 62 22 0d 0a 41 63   ceedc3cb 79b"··Ac
00e0  63 65 70 74 2d 52 61 6e  67 65 73 3a 20 62 79 74   cept-Ran ges: byt
00f0  65 73 0d 0a 43 6f 6e 74  65 6e 74 2d 4c 65 6e 67   es··Cont ent-Leng
0100  74 68 3a 20 31 39 30 0d  0a 4b 65 65 70 2d 41 6c   th: 190· ·Keep-Al
0110  69 76 65 3a 20 74 69 6d  65 6f 75 74 3d 35 2c 20   ive: tim eout=5,
0120  6d 61 78 3d 31 30 30 0d  0a 43 6f 6e 6e 65 63 74   max=100· ·Connect
0130  69 6f 6e 3a 20 4b 65 65  70 2d 41 6c 69 76 65 0d   ion: Kee p-Alive·
0140  0a 0d 0a 0a 0a 0a 4b 45  59 4b 45 59 31 20 53 45   ······KE YKEY1 SE
0150  4e 44 20 31 35 35 35 35  32 31 35 35 35 36 20 59   ND 15555 215556 Y
0160  6f 75 20 68 61 76 65 20  62 65 65 6e 20 69 6e 20   ou have  been in
0170  63 6c 6f 73 65 20 63 6f  6e 74 61 63 74 20 77 69   close co ntact wi
0180  74 68 20 73 6f 6d 65 6f  6e 65 20 77 68 6f 20 68   th someo ne who h
0190  61 73 20 43 4f 56 49 44  2d 31 39 2e 20 54 61 70   as COVID -19. Tap
```

wireshark_VirtualBox Host-Only Network #17MM5QK1.pcapng | Packets: 11853 · Displayed: 596 (5.0%) | Profile: Default

Figure 25a - The traffic captured by Wireshark



```
> Frame 6584: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface \Device\NPF_{CE4DB711-DC11-45B2-BB24-18710A5F1B6C}, id 0
> Ethernet II, Src: PcsCompu_76:73:6d (08:00:27:76:73:6d), Dst: 0a:00:27:00:00:1f (0a:00:27:00:00:1f)
> Internet Protocol Version 4, Src: 192.168.37.104, Dst: 192.168.37.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 7322, Seq: 1, Ack: 196, Len: 459
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Mon, 18 Apr 2022 14:41:58 GMT\r\n
    Server: Apache/2.4.6 (CentOS) PHP/5.5.21\r\n
    Last-Modified: Mon, 18 Apr 2022 14:40:58 GMT\r\n
    ETag: "be-5dceebfa07f9b"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 190\r\n
```

```
0090  35 2e 32 31 0d 0a 4c 61  73 74 2d 4d 6f 64 69 66   5.21··La st-Modif
00a0  69 65 64 3a 20 4d 6f 6e  2c 20 31 38 20 41 70 72   ied: Mon , 18 Apr
00b0  20 32 30 32 32 20 31 34  3a 34 30 3a 35 38 20 47    2022 14 :40:58 G
00c0  4d 54 0d 0a 45 54 61 67  3a 20 22 62 65 2d 35 64   MT··ETag : "be-5d
00d0  63 65 65 62 66 61 30 37  66 39 62 22 0d 0a 41 63   ceebfa07 f9b"··Ac
00e0  63 65 70 74 2d 52 61 6e  67 65 73 3a 20 62 79 74   cept-Ran ges: byt
00f0  65 73 0d 0a 43 6f 6e 74  65 6e 74 2d 4c 65 6e 67   es··Cont ent-Leng
0100  74 68 3a 20 31 39 30 0d  0a 4b 65 65 70 2d 41 6c   th: 190· ·Keep-Al
0110  69 76 65 3a 20 74 69 6d  65 6f 75 74 3d 35 2c 20   ive: tim eout=5,
0120  6d 61 78 3d 31 30 30 0d  0a 43 6f 6e 6e 65 63 74   max=100· ·Connect
0130  69 6f 6e 3a 20 4b 65 65  70 2d 41 6c 69 76 65 0d   ion: Kee p-Alive·
0140  0a 0d 0a 0a 0a 0a 4b 45  59 4b 45 59 31 20 53 45   ······KE YKEY1 SE
0150  4e 44 20 31 35 35 35 35  32 31 35 35 35 36 20 59   ND 15555 215556 Y
0160  6f 75 20 68 61 76 65 20  62 65 65 6e 20 69 6e 20   ou have  been in
0170  63 6c 6f 73 65 20 63 6f  6e 74 61 63 74 20 77 69   close co ntact wi
0180  74 68 20 73 6f 6d 65 6f  6e 65 20 77 68 6f 20 68   th someo ne who h
0190  61 73 20 43 4f 56 49 44  2d 31 39 2e 20 54 61 70   as COVID -19. Tap
01a0  20 68 65 72 65 20 66 6f  72 20 6d 6f 72 65 20 64    here fo r more d
```

Figure 25b - HTTP communication after resolved to the Dagah server

5. RECOMMENDATIONS

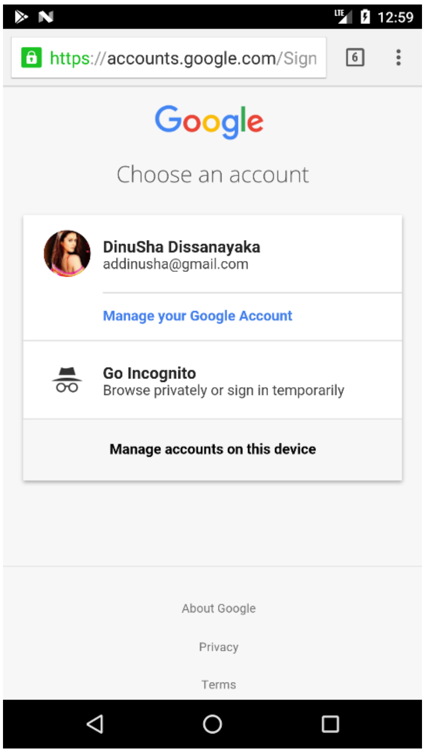
Defense against Dagah type social engineering attacks via SMS

5.2 Gmail credential harvesting

The only method to protect people from social engineering attacks is to raise their awareness. When someone receives such an SMS, they should not act on it right away; instead, they should carefully examine it, verify it, and then proceed.

- Understanding the suspicious behaviour is important since Gmail never requests that suspicious logging activity be checked via SMS. They will only notify you via email. As a result, in the beginning, we should ignore and delete this type of suspicious SMS.

- When victims clicked the malicious link and were redirected to the phony Gmail login, we can see some information about the malicious behaviour in the address bar of the web page, as shown in Figure 20. The information "https://accounts.google.com/signin" is always displayed in the address bar of a valid Gmail login page, as seen in Figure 26. Therefore, they should double-check it before inputting their credentials. The information in the address bar of the phony Gmail login page is completely different from the actual page.



12:59

https://accounts.google.com/Sign

Google

Choose an account

DinuSha Dissanayaka
addinusha@gmail.com

Manage your Google Account

Go Incognito
Browse privately or sign in temporarily

Manage accounts on this device

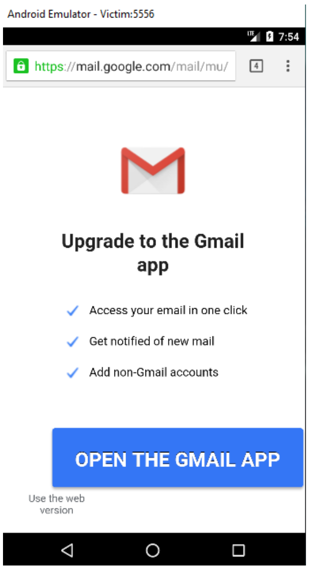
About Google

Privacy

Terms

Figure 26 – Original Gmail login page

- If the victim enters his credentials on the fake Gmail login page, then they will be sent to another general Gmail page rather than being logged into their Gmail accounts (as in Figure 27). So, the victim should be aware of this unusual behaviour and change their Gmail account password right once to avoid additional harm.



Android Emulator - Victim:5556

7:54

https://mail.google.com/mail/mu/

Upgrade to the Gmail app

✓ Access your email in one click

✓ Get notified of new mail

✓ Add non-Gmail accounts

OPEN THE GMAIL APP

Use the web version

Figure 27 - General Gmail page receives after entering credentials on the fake Gmail login page

- Multi-factor authentication can be used (MFA). If the account being hacked requires a second "key" for verification, a revealed password may still be useless to a smishing attacker. Two-factor authentication (2FA), which frequently employs a text message verification code, is the most used MFA option. Stronger options include employing a dedicated verification app (such as Google Authenticator).

- If a message is urgent, take it slowly. Urgent account upgrades and limited-time offers should be treated as red flags of likely smishing. Maintain your skepticism and continue with caution.

5.2 Installing malicious software on victim’s mobile phone

- Understanding the suspicious behaviour would also be beneficial in this scenario. Normally, any kind of Covid or health-related information is not sent by private numbers. Email-to-text services can be identified by odd-looking phone numbers, such as 4-digit ones. There should be a recognized name such as NHS, GP, etc. Still, if someone feels suspicious about any text message, it is better to confirm it by calling their official number directly (NHS, GP centre’s number, etc).

- We should be very wary of SMSs that ask us to install something on our phone, and we should not click on these links in the first place.

- We should only install software created by reputable publishers and obtained from reputable sources such as Google's Play Store, Apple's App Store, and others.

- Keep credit card numbers off your phone if at all possible. The greatest method to avoid having financial information stolen from a digital wallet is to never put it there in the first place.

Unsolved Problems

- CTI is not yet developed enough to be deployed fully and successfully, for most of the sectors [24].

- Due to the evolving of CTI standards, it is expensive, complex, and complicated for businesses to implement and stay up with this technology.
- Developing good quality CTI necessitates a successful collaborative venture, but the difficulty is that enterprises are typically hesitant to share information regarding security breaches, resulting in a significant information gap and poor threat intelligence [24].

6. CONCLUSION

We observed that the technique utilised for both compromises in the above demonstration scenario was two Social Engineering attacks via SMS. Even if an organisation has strong and effective Cybersecurity controls in place, a small lapse can result in a major disaster because if just one employee within the organisation clicks on a malicious link or downloads an infected file from a spear-phishing text message, the entire organisational network can be infected and become a victim of a massive attack. Because humans are the weakest link in the cybersecurity chain [25], it is critical that businesses raise employee knowledge of everyday social engineering attacks through effective training and the development of comprehensive information security policies. Organizational-level Social Engineering exercises should be undertaken on a regular basis, imitating real-world attack scenarios.

REFERENCES

[1] National Cyber Security Centre, "Phishing: Spot and report scam emails, texts, websites and calls," 26 11 2021. [Online]. Available: https://www.ncsc.gov.uk/collection/phishing-scams.

[2] proofpoint, "Security Brief: Mobile Phishing Increases More Than 300% as 2020 Chaos Continues," 02 11 2020. [Online]. Available: https://www.proofpoint.com/us/blog/threat-protection/mobile-phishing-increases-more-300-2020-chaos-continues.

[3] Kaspersky, "SMS Attacks and SMS Mobile Threats," [Online]. Available: https://www.kaspersky.com/resource-center/threats/sms-attacks.

[4] National Cyber Security Centre, Government Counter Fraud Function, "COVID-19: SMS / Text message SCAMS," United Kingdom, 2020.

[5] nextcaller, "Pindrop Acquires Next Caller," 2021.

[6] B. Martens, "11 Facts + Stats on Smishing (SMS Phishing) in 2022," 2022. [Online]. Available: https://www.safetydetectives.com/blog/what-is-smishing-sms-phishing-facts/.

[7] Ofcom, "Coronavirus scam calls and texts," 2022.

[8] S. A. Ikechukwu Ibekwe, "SMS Security: Highlighting Its Vulnerabilities & Techniques Towards Developing a Solution," University of Portsmouth, United Kingdom.

[9] Twitter Inc., "An update on our security incident," 18 07 2020. [Online]. Available: https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.

[10] W. W. C. W. J. C. C. Q. T. J. L. Z. K. L. X. L. Y. L. Zhenhua Li, "FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild," NDSS, 2017.

[11] Sohu Media Platform, "Demystifying the Industrial Chain of Fake Base," 2016.

[12] B. L. C. L. Z. L. H. D. S. H. M. L. Y. L. D. W. Q. L. Yiming Zhang, " Lies in the Air: Characterizing Fake-base-station Spam Ecosystem in China," Proceedings of the 2020 ACM, 2020.

[13] L. B. D. T. P. T. K. R. B. Bradley Reaves, "Detecting SMS spam in the age of legitimate bulk messaging," The 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, 2016.

[14] N. S. D. T. L. B. P. T. K. R. B. Bradley Reaves, "Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways," 2016 IEEE Symposium on Security, 2016.

[15] P. G. Baris Coskun, "Mitigating sms spam by online detection of repetitive near-duplicate messages," IEEE International Conference on Communications (ICC), 2012.

[16] G. C. B. E. P. S. F. C. G. José María Gómez Hidalgo, "Content based SMS spam filtering," The 2006 ACM symposium on Document engineering, 2006.

[17] R. P. J. Ilona Murynets, "How an SMS-Based malware infection will get throttled by the wireless link," IEEE International Conference, 2012.

[18] N. Zablotskaya, "Fraudulent spam," 2008.

[19] J. M. G. H. A. Y. Tiago A Almeida, "Contributions to the study of SMS spam filtering: new collection and results," The 11th ACM symposium on Document engineering, 2011.

[20] J. M. G. H. E. P. S. Gordon V Cormack, "Spam filtering for short messages," the sixteenth ACM conference on Conference on information and knowledge management, 2007.

[21] Y. Z. J. L. K. Y. X. W. Jialin Ma, "Intelligent SMS spam filtering using topic model," International Conference on Intelligent Networking and Collaborative Systems (INCoS), 2016.

[22] Y. Z. Y. T. P. C. Rui Li, "A novel method for detecting telecom fraud user," 3rd International Conference on Information Systems Engineering (ICISE), 2018.

[23] Kaspersky, "What is Smishing and How to Defend Against it," 2020. [Online]. Available: https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it.

[24] S. R. S. A. A. R. Y. M. S. Abu, "Cyber threat intelligence–issue and challenges," Indonesian Journal of Electrical Engineering and Computer Science, 2018.

[25] B. Schneier, "Secrets and Lies: Digital Security in a Networked World," 2000.