Fast Flux Networks

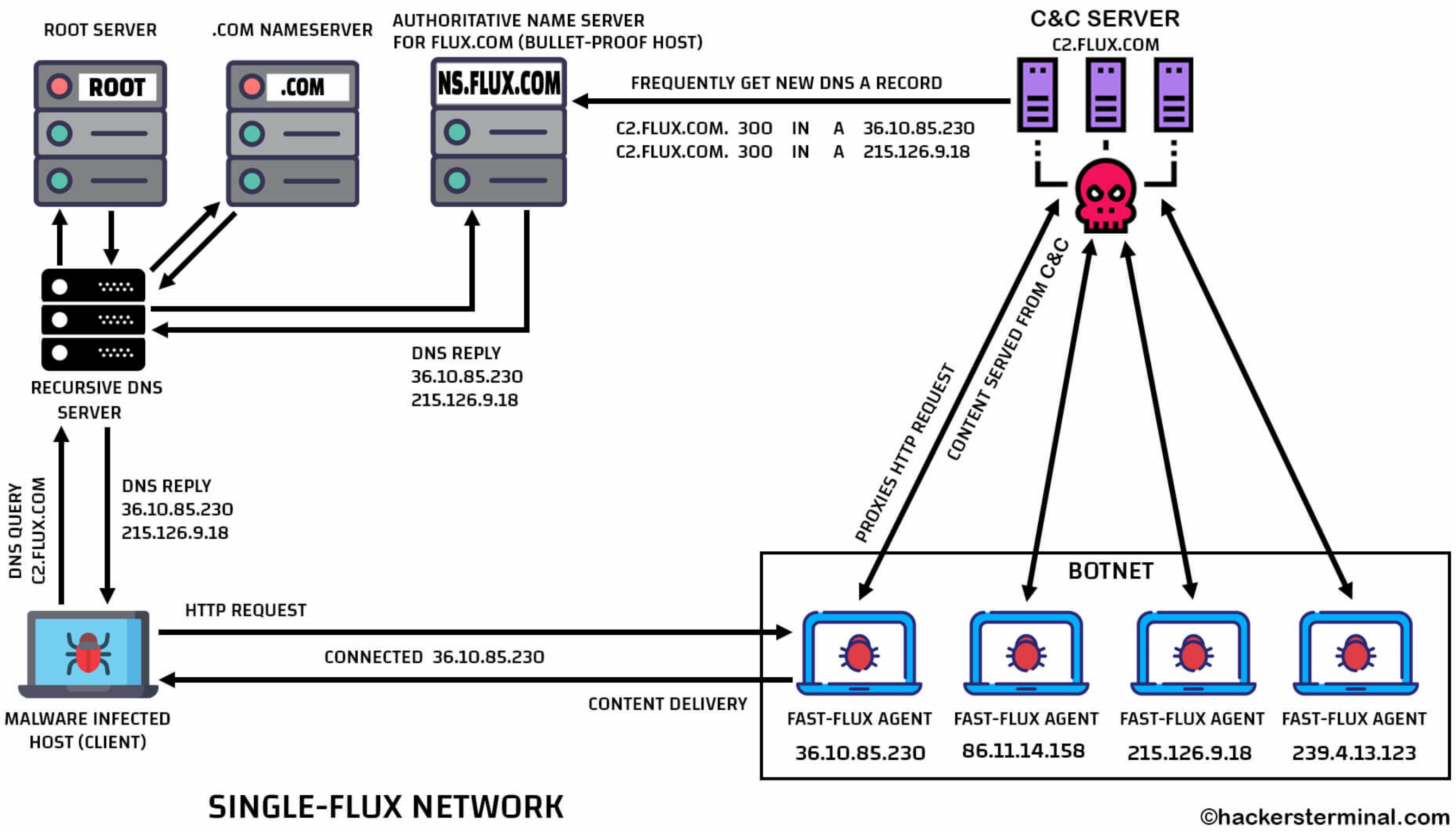
THE TERM FAST FLUX CAN REFER TO NETWORKS USED BY SEVERAL BOTNETS TO HIDE THE DOMAINS USED TO DOWNLOAD MALWARE OR HOST PHISHING WEBSITES

Fast Flux Networks in Details

- **Types of Fast Flux Networks**

- 1.) **Single Fast-Flux :** This is achieved by changing the A records rapidly with less than 300 TTL usually.

- 2.) **Double Fast-Flux :** A more sophisticated type of fast flux, referred to itself as "double-flux", is characterized by multiple nodes within the network registering and de-registering their addresses as part of the DNS Name Server record list for the DNS zone.



Credit : https://hackersterminal.com/fast-flux-service-networks-ffsn-technique/

List of Platforms/Software used

- Here is the list which I have used to demonstrate the working of Fast Flux Networks.

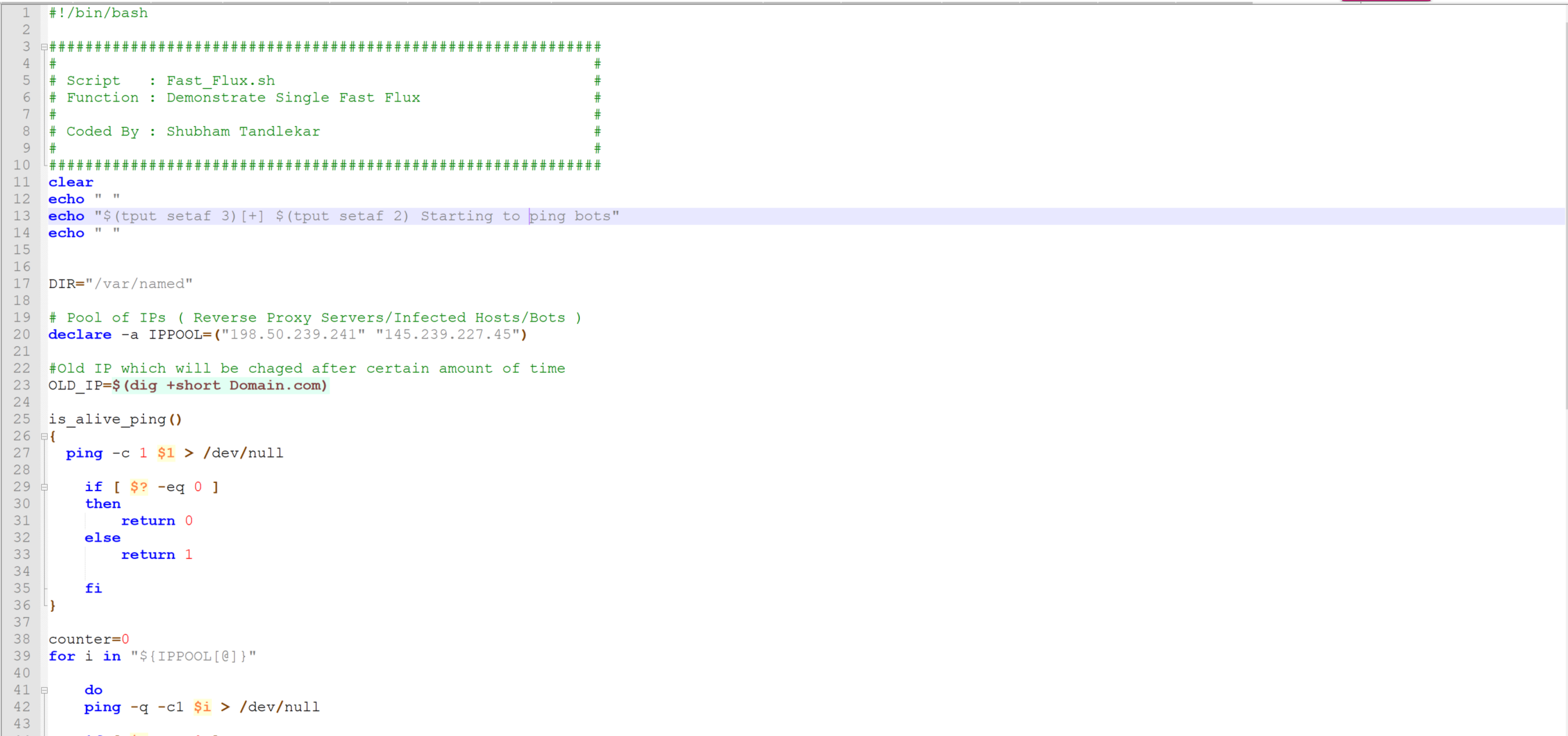
- 1.) WHM/cPanel – (Acting as a DNS Server)
- 2.) Nginx – (Reverse Proxies)
- 3.) Cron – (Software Utility to run your scripts in given intervals)
- 4.) LAMP
- 5.) Bash Scripts

Conditions :

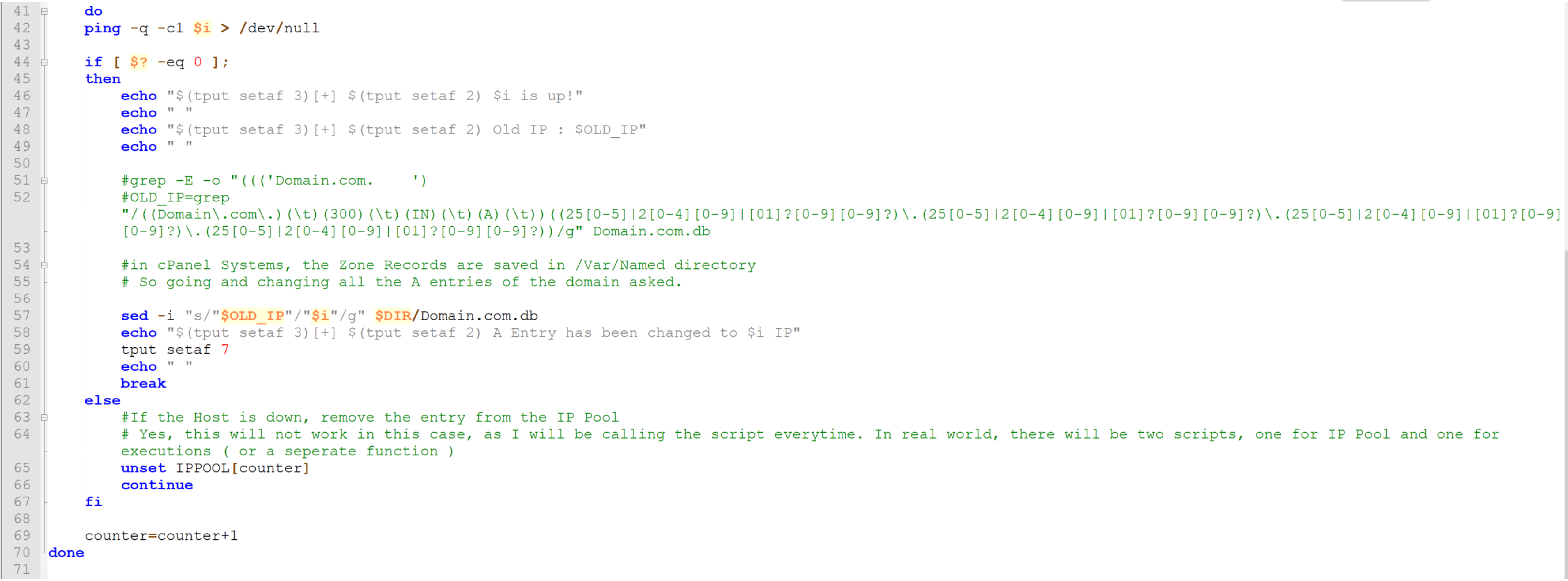
- 1.) Single Fast Flux networks change their IP rapidly without waiting for anything but for demonstration purposes, I had modified this concept by a bit. My Script changes IP only when proxy/Bot from the IP Pool goes down and not unless. (Which is a good thing as it does not reveal all the IPs and hence helps the attacker achieve their goal).

- 2.) I had to sync the DNS Records manually because I had 10 secs to show the updated A record for that domain. (TTL was 100). This helped me clear my local DNS Cache and update it with the latest IP and hence to speed up the whole process.

Code : Fast_Flux.sh



```
#!/bin/bash

###############################################################
#                                                             #
# Script   : Fast_Flux.sh                                     #
# Function : Demonstrate Single Fast Flux                     #
#                                                             #
# Coded By : Shubham Tandlekar                                #
#                                                             #
###############################################################
clear
echo " "
echo "$(tput setaf 3)[+] $(tput setaf 2) Starting to ping bots"
echo " "


DIR="/var/named"

# Pool of IPs ( Reverse Proxy Servers/Infected Hosts/Bots )
declare -a IPPOOL=("198.50.239.241" "145.239.227.45")

#Old IP which will be chaged after certain amount of time
OLD_IP=$(dig +short Domain.com)

is_alive_ping()
{
  ping -c 1 $1 > /dev/null

    if [ $? -eq 0 ]
    then
        return 0
    else
        return 1

    fi
}

counter=0
for i in "${IPPOOL[@]}"

    do
    ping -q -c1 $i > /dev/null

```



```
    do
    ping -q -c1 $i > /dev/null

    if [ $? -eq 0 ];
    then
        echo "$(tput setaf 3)[+] $(tput setaf 2) $i is up!"
        echo " "
        echo "$(tput setaf 3)[+] $(tput setaf 2) Old IP : $OLD_IP"
        echo " "

        #grep -E -o "((('Domain.com.    ')
        #OLD_IP=grep "/((Domain\.com\.)(\t)(300)(\t)(IN)(\t)(A)(\t))((25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))/g" Domain.com.db

        #in cPanel Systems, the Zone Records are saved in /Var/Named directory
        # So going and changing all the A entries of the domain asked.

        sed -i "s/"$OLD_IP"/"$i"/g" $DIR/Domain.com.db
        echo "$(tput setaf 3)[+] $(tput setaf 2) A Entry has been changed to $i IP"
        tput setaf 7
        echo " "
        break
    else
        #If the Host is down, remove the entry from the IP Pool
        # Yes, this will not work in this case, as I will be calling the script everytime. In real world, there will be two scripts, one for IP Pool and one for executions ( or a seperate function )
        unset IPPOOL[counter]
        continue
    fi

    counter=counter+1
done

```

Why it is so hard to stop them

- **Reasons :**

- 1.) The systems in the network have multiple IP addresses from multiple ISPs and exist on multiple physical networks, probably all over the world.
- 2.) IP Pool System (The Flux)
- 3.) The DNS entries for the network have very low TTLs (this is the "time to live" value; a low value means that the entries won't be long-cached and the servers will be rechecked frequently)
- 4.) The whole network is self-contained; the hosts, the proxies, the DNS servers, all run on the botnet.

Why it is so hard to stop them

- 5.) IP Spoofing (500 Fortune Companies and legit sources)
- 6.) The NS (name server) entries in the registration themselves get fluxed.

Profit Calculations :

- **Case : A Spammer**
- **Cost Involved :**

- **1.)** LAMP Server – 40-50$
- **2.)** Nginx Server – 5-7$ per Server
- **3.)** cPanel License – 15$
- **4.)** A Backup Server – 20$

- 1x LAMP – 50$ + 10x Nginx Servers – 50$ + cPanel License = ~**150$**

Profit Calculations :

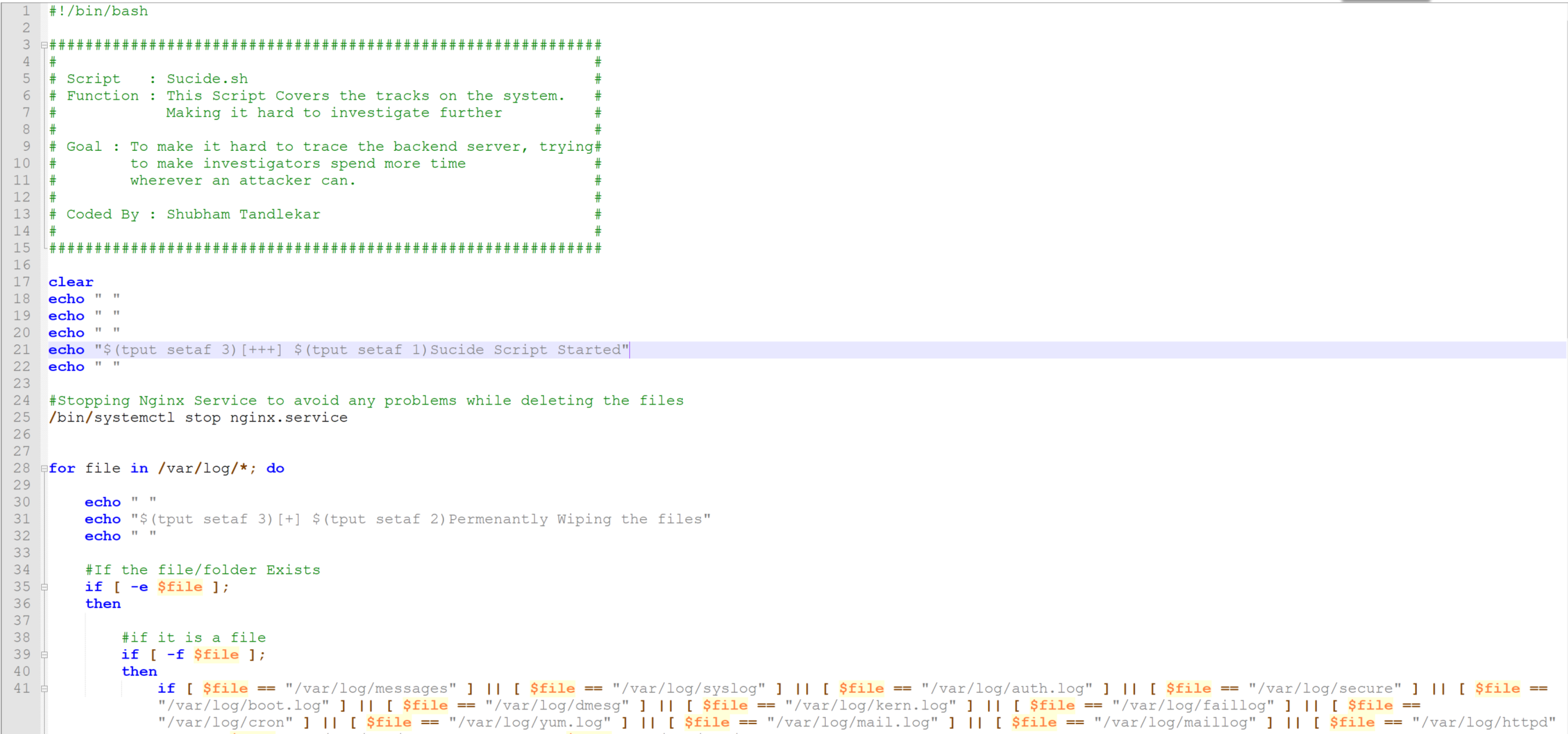
- **Actual Profit Margin :**

- Your Host is staying up for say 1 day (which is not the real case) :
- You are sending **1,000,000 (1M) Emails (i.e ~42,000 emails an hour)**
- **10%** - Saw the email and Replied
- **1%** - Actually became the victim
- If you are earning **100$ from a victim** then **1% of 1M is 10,000**

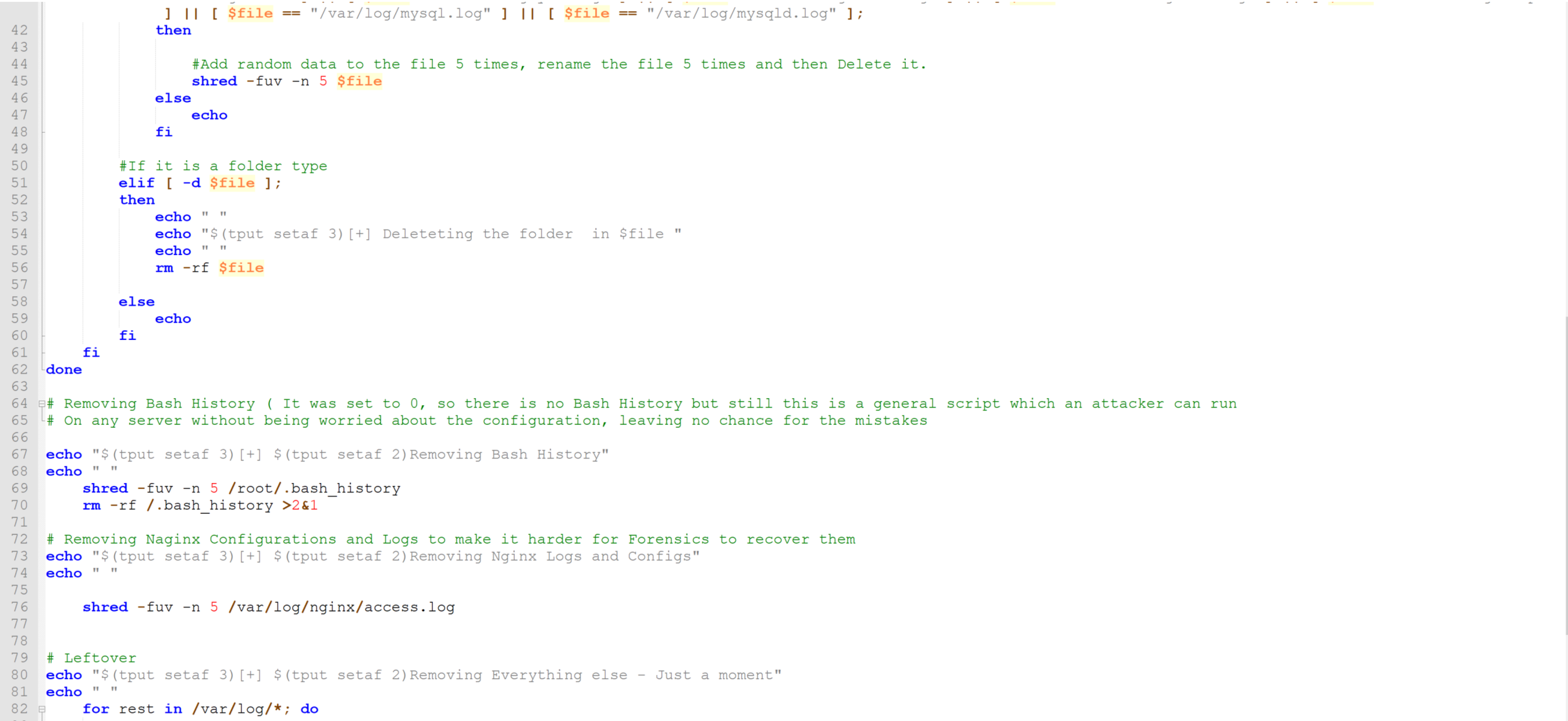
- **Profit** = 10,000 x100$ = **~1,000,000 USD (1 Million USD – 150 USD :p)** just in a day!

Note : It is not a good advice to spam 1,000,000 Emails from a single domain within a day. It will surely make your domain/IPs list in Blacklists. This game is played at the slower rate.

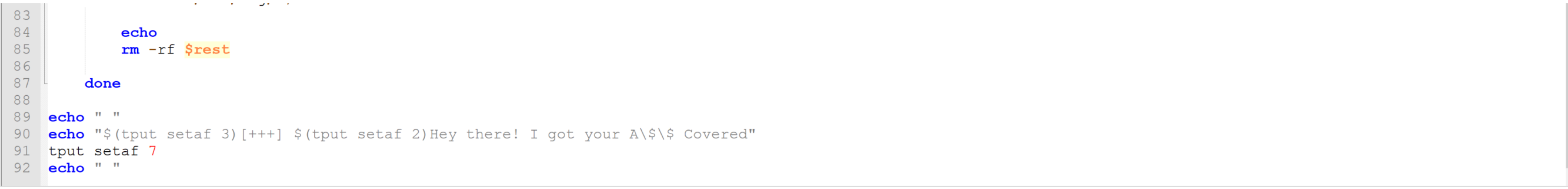
Code of Sucide.sh



```bash
#!/bin/bash

##############################################################
#                                                            #
# Script   : Sucide.sh                                       #
# Function : This Script Covers the tracks on the system.    #
#            Making it hard to investigate further           #
#                                                            #
# Goal : To make it hard to trace the backend server, trying#
#        to make investigators spend more time               #
#        wherever an attacker can.                           #
#                                                            #
# Coded By : Shubham Tandlekar                                #
#                                                            #
##############################################################

clear
echo " "
echo " "
echo " "
echo "$(tput setaf 3)[+++] $(tput setaf 1)Sucide Script Started"
echo " "

#Stopping Nginx Service to avoid any problems while deleting the files
/bin/systemctl stop nginx.service


for file in /var/log/*; do

    echo " "
    echo "$(tput setaf 3)[+] $(tput setaf 2)Permenantly Wiping the files"
    echo " "

    #If the file/folder Exists
    if [ -e $file ];
    then

        #if it is a file
        if [ -f $file ];
        then
            if [ $file == "/var/log/messages" ] || [ $file == "/var/log/syslog" ] || [ $file == "/var/log/auth.log" ] || [ $file == "/var/log/secure" ] || [ $file ==
            "/var/log/boot.log" ] || [ $file == "/var/log/dmesg" ] || [ $file == "/var/log/kern.log" ] || [ $file == "/var/log/faillog" ] || [ $file ==
            "/var/log/cron" ] || [ $file == "/var/log/yum.log" ] || [ $file == "/var/log/mail.log" ] || [ $file == "/var/log/maillog" ] || [ $file == "/var/log/httpd"
```



```
             ] || [ $file == "/var/log/mysql.log" ] || [ $file == "/var/log/mysqld.log" ];
            then

                #Add random data to the file 5 times, rename the file 5 times and then Delete it.
                shred -fuv -n 5 $file
            else
                echo
            fi

        #If it is a folder type
        elif [ -d $file ];
        then
            echo " "
            echo "$(tput setaf 3)[+] Deleteting the folder  in $file "
            echo " "
            rm -rf $file

        else
            echo
        fi
    fi
done

# Removing Bash History ( It was set to 0, so there is no Bash History but still this is a general script which an attacker can run
# On any server without being worried about the configuration, leaving no chance for the mistakes

echo "$(tput setaf 3)[+] $(tput setaf 2)Removing Bash History"
echo " "
    shred -fuv -n 5 /root/.bash_history
    rm -rf /.bash_history >2&1

# Removing Naginx Configurations and Logs to make it harder for Forensics to recover them
echo "$(tput setaf 3)[+] $(tput setaf 2)Removing Nginx Logs and Configs"
echo " "

    shred -fuv -n 5 /var/log/nginx/access.log


# Leftover
echo "$(tput setaf 3)[+] $(tput setaf 2)Removing Everything else - Just a moment"
echo " "
    for rest in /var/log/*; do
```



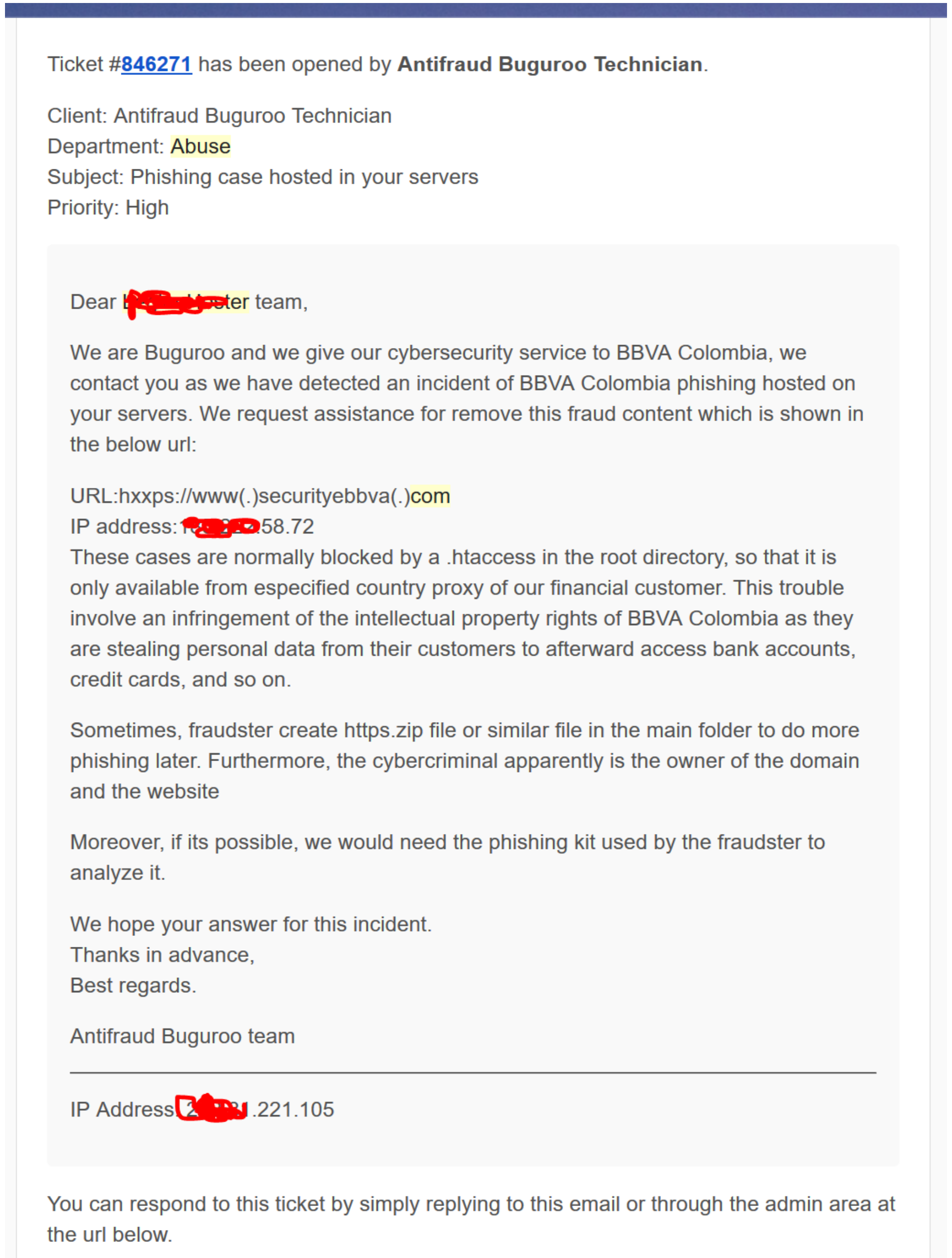
```
        echo
        rm -rf $rest

    done

echo " "
echo "$(tput setaf 3)[+++] $(tput setaf 2)Hey there! I got your A\$\$ Covered"
tput setaf 7
echo " "
```

Assumptions:

- 1.) There are thousands of way an attacker can get caught. (So called ”Digital Footprints”) but the Sucide.sh script demonstrates what can be done on the host to cover the tracks. This plays an important role for post-investigations when Agencies try to reverse the attacks and try to understand how it was executed. It is very common for investigators to ask for backup of the server.

- 2.) I know a lot Small to Medium Size Hosting companies check the servers after receving abuse report and if they actually find such configurations, they report it back to Agencies/Blacklists/Or_Whoever_Reports. This is a fact and I have seen it so many times. (This is not the case with big Fishes though but why an attacker would like to buy a server from Amazon and not from a Bulletproof Hosting provider?)

Report 1 :



Ticket #846271 has been opened by **Antifraud Buguroo Technician**.

Client: Antifraud Buguroo Technician
Department: Abuse
Subject: Phishing case hosted in your servers
Priority: High

Dear [redacted]ter team,

We are Buguroo and we give our cybersecurity service to BBVA Colombia, we contact you as we have detected an incident of BBVA Colombia phishing hosted on your servers. We request assistance for remove this fraud content which is shown in the below url:

URL:hxxps://www(.)securityebbva(.)com
IP address:[redacted]58.72
These cases are normally blocked by a .htaccess in the root directory, so that it is only available from especified country proxy of our financial customer. This trouble involve an infringement of the intellectual property rights of BBVA Colombia as they are stealing personal data from their customers to afterward access bank accounts, credit cards, and so on.

Sometimes, fraudster create https.zip file or similar file in the main folder to do more phishing later. Furthermore, the cybercriminal apparently is the owner of the domain and the website

Moreover, if its possible, we would need the phishing kit used by the fraudster to analyze it.

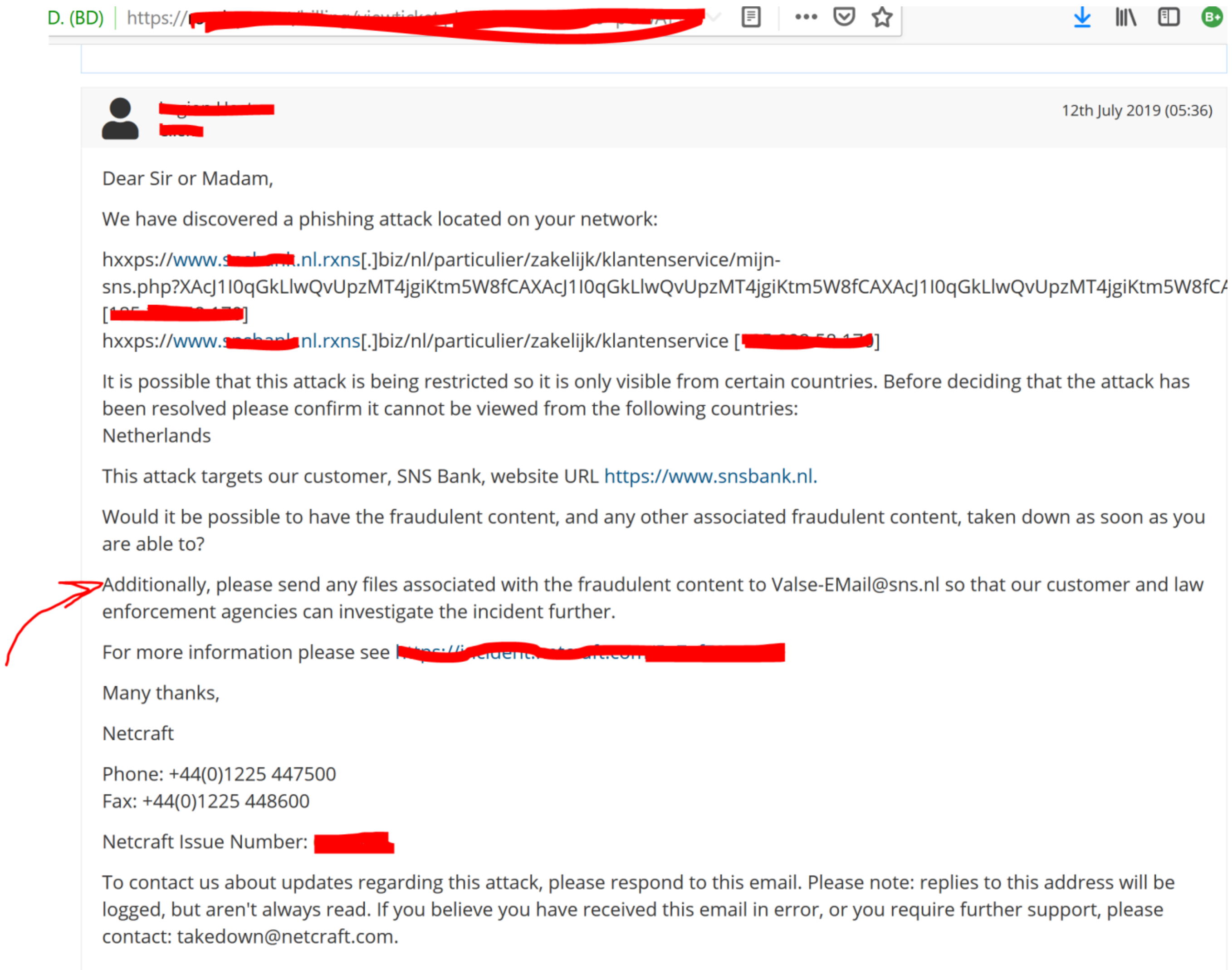
We hope your answer for this incident.
Thanks in advance,
Best regards.

Antifraud Buguroo team

IP Address[redacted].221.105

You can respond to this ticket by simply replying to this email or through the admin area at the url below.

Report 2 :



D. (BD) | https://[redacted]

[redacted]

12th July 2019 (05:36)

Dear Sir or Madam,

We have discovered a phishing attack located on your network:

hxxps://www.s[redacted].nl.rxns[.]biz/nl/particulier/zakelijk/klantenservice/mijn-sns.php?XAcJ1I0qGkLlwQvUpzMT4jgiKtm5W8fCAXAcJ1I0qGkLlwQvUpzMT4jgiKtm5W8fCAXAcJ1I0qGkLlwQvUpzMT4jgiKtm5W8fCA
[[redacted]]
hxxps://www.s[redacted].nl.rxns[.]biz/nl/particulier/zakelijk/klantenservice [[redacted]]

It is possible that this attack is being restricted so it is only visible from certain countries. Before deciding that the attack has been resolved please confirm it cannot be viewed from the following countries:
Netherlands

This attack targets our customer, SNS Bank, website URL https://www.snsbank.nl.

Would it be possible to have the fraudulent content, and any other associated fraudulent content, taken down as soon as you are able to?

Additionally, please send any files associated with the fraudulent content to Valse-EMail@sns.nl so that our customer and law enforcement agencies can investigate the incident further.

For more information please see [redacted]

Many thanks,

Netcraft

Phone: +44(0)1225 447500
Fax: +44(0)1225 448600

Netcraft Issue Number: [redacted]

To contact us about updates regarding this attack, please respond to this email. Please note: replies to this address will be logged, but aren't always read. If you believe you have received this email in error, or you require further support, please contact: takedown@netcraft.com.

Covering the tracks/Sucide

- **The Plan :**

- 1.) Use Different BulletProof Hosting Providers
- 2.) Encrypt the Drives (If you can)
- 3.) Use Proxies/VPN while contacting to the Servers/ClientArea
- 4.) Use Cryptos for purchasing (Using Anonymizing Services)
- 5.) Create Triggers for your Sucide.sh Script

Final Quote

Anonymity is a calculated risk!

Calculate it right!

Detailed Analysis of Fast Flux Networks

- **AKAMAI :** https://www.akamai.com/uk/en/multimedia/documents/white-paper/digging-deeper-in-depth-analysis-of-fast-flux-network.pdf
- **WikiPedia :** https://en.wikipedia.org/wiki/Fast_flux

```
___________.__                   __       _____.___.
\__    ___/|  |__ _____    ____ |  | __   \__  |   | ____  __ __
  |    |   |  |  \\__  \  /    \|  |/ /    /   |   |/  _ \|  |  \
  |    |   |   Y  \/ __ \|   |  \    <     \____   (  <_> )  |  /
  |____|   |___|  (____  /___|  /__|_ \    / ______|\____/|____/
                \/     \/     \/     \/    \/
```