Android FluBot enters Switzerland

securityblog.switch.ch/2021/06/19/android-flubot-enters-switzerland/

June 19, 2021

FluBot is a new Android malware first discovered in December 2020. During the first few months, FluBot has been active in Spain, Hungary and Poland. Since then, the development of the malware advanced quickly and the malware has set foot in almost all European countries.

On the 18th of June 2021 FluBot version 4.6 was spotted which added a configuration for Switzerland. As of today it is actively being spamertized through SMS.

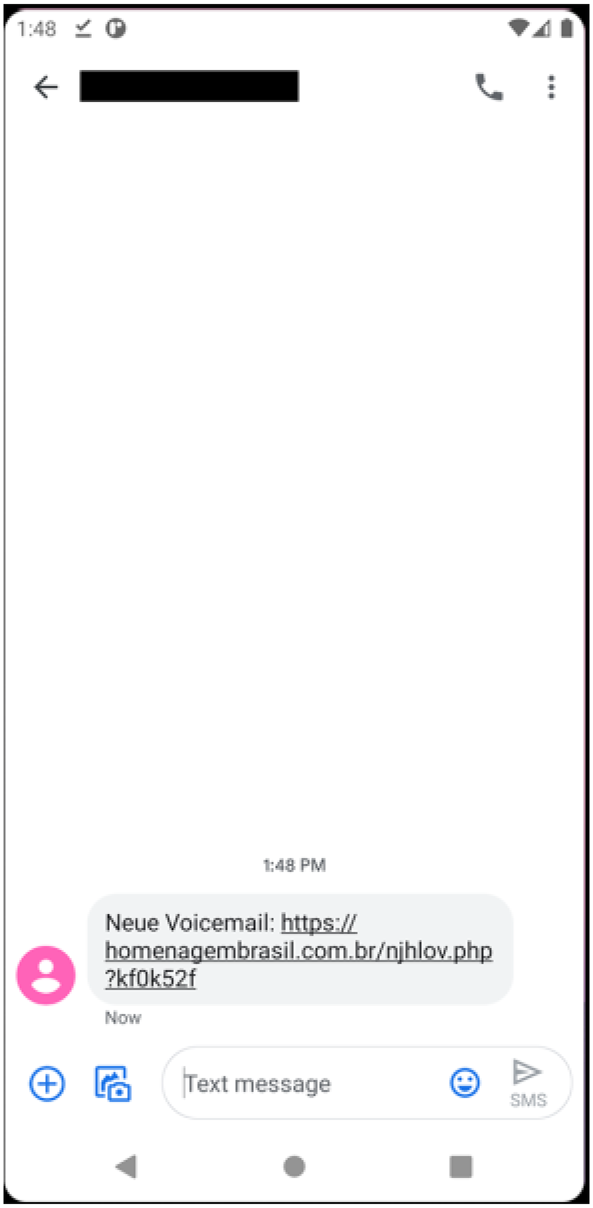
Alias Names

FluBot is known by different names. The name “FluBot” is best known because this was the name given in the first public technical writing. Below the reference to the most well known aliases:

- January 2021, ThreatFabric was the first to give it the name “**Cabassous**” in a Twitter post
- March 2021, ProDaft published a detailed technical report and gave it the name **“FluBot”**
- April 2021, IBM Trusteer took a deeper look at the different FluBot versions and gave it the name “**FakeChat**“

Distribution

FluBot is distributed using smishing (a combination from the words SMS and phishing). The victim receives an SMS with a link to an URL which distributes the APK. The installation is straight forward using sideloading.

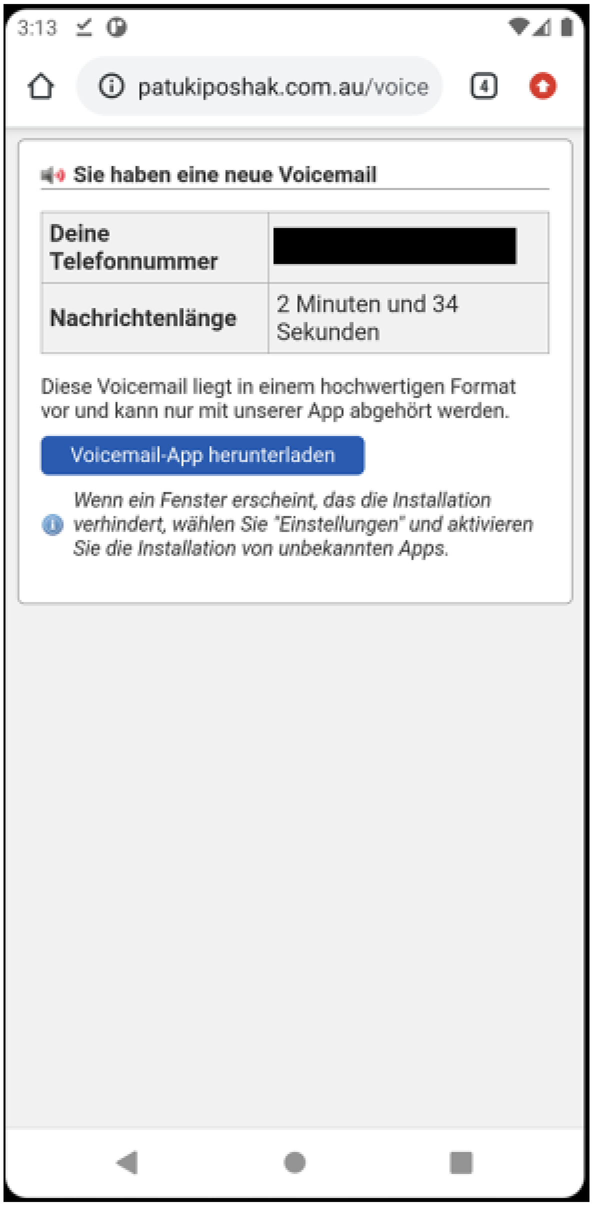


[redacted]

1:48 PM

Neue Voicemail: https://homenagembrasil.com.br/njhlov.php?kf0k52f

Now



Sie haben eine neue Voicemail

Deine Telefonnummer	[redacted]
Nachrichtenlänge	2 Minuten und 34 Sekunden

Diese Voicemail liegt in einem hochwertigen Format vor und kann nur mit unserer App abgehört werden.

Wenn ein Fenster erscheint, das die Installation verhindert, wählen Sie "Einstellungen" und aktivieren Sie die Installation von unbekannten Apps.

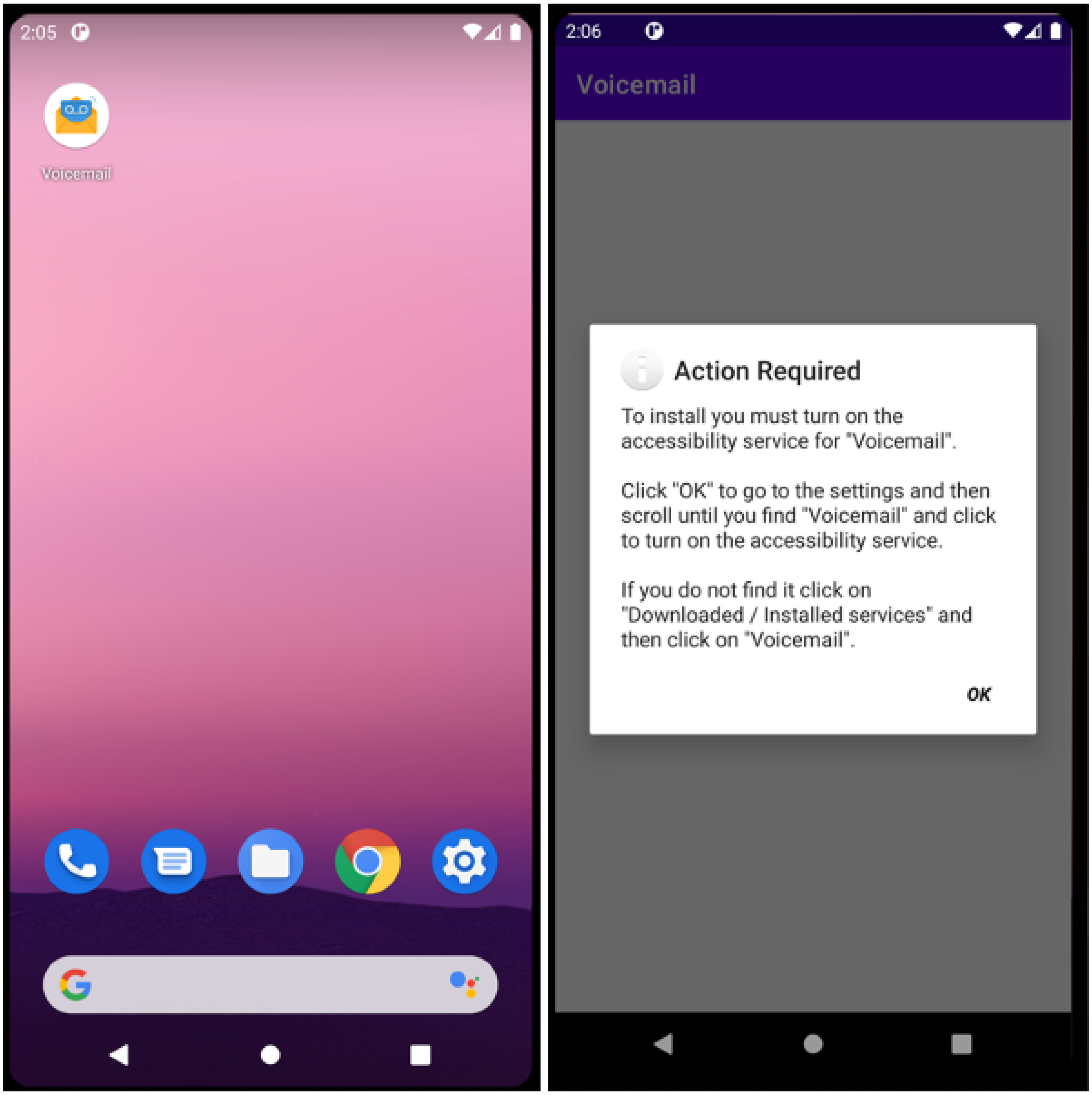
If the recipient device is not an Android mobile phone or the fraudster does not want to distribute the malware at that time, the URL redirects the user to a scam website or with the Voicemail lure we have seen a redirection to the Voicemail app from Deutsche Telekom AG on the Google Playstore.

FluBot SMS are typically sent from other infected mobile phones. If the number of infected devices within a country is not very high it has been seen that infected devices from other countries are used to send the SMS.

The SMS text message may vary as do the URLs. Sometimes they talk about parcel delivery using brands such as DHL or UPS. The current campaign in Switzerland uses Voicemail as a lure. The malware distributed in Switzerland from the smishing URLs are currently all FluBot samples. However, this may change as in other countries it has been seen that another well known trojan called Anatsa is dropped instead. See also tweet by ThreatFabric.

Installation

Once installed and started, FluBot asks for Accessibility Service permission (Screenshot on the right side). This permission is normally used by apps to help users with disabilities to use a mobile device. However, if granted to FluBot, it can control the mobile device as if done by a normal user. First, it will grant itself additional permissions automatically. For example, it will set itself as the **default SMS application**, grant itself access to **read the phone book, read or block notifications** and more. Secondly, Accessibility Service is also used to prevent the user from uninstalling the malware. The user has to boot into “Safe Mode” in order to uninstall it. Third and finally, it uses accessibility permission to monitor the device usage and e.g. start overlays if for example targetted app is started. The overlay, because started a fraction of a second later, will take over the screen and trick the user into enter credentials or other sensitive information.



Action Required

To install you must turn on the accessibility service for "Voicemail".

Click "OK" to go to the settings and then scroll until you find "Voicemail" and click to turn on the accessibility service.

If you do not find it click on "Downloaded / Installed services" and then click on "Voicemail".

The installed FluBot app has no user interface for the user. If the user starts the app a short message appears informing the user that the installation failed.

Network Communication

FluBot uses a Domain-Generation-Algorithm (DGA) to find the command and control (c2) server domain name. The DGA generates 5000 domain names per month and uses different seeds. The following DGA seeds have been observed over time:

- 1136 (+34 ES)
- 1642 (+44 UK)
- 1813 (+39 IT)
- 1905 (+81 JP)
- 1945 (+41 de-CH, +43 AT, +49 DE)
- 1949 (+36 HU)
- 2931 (+30 GR, +31 NL, +32 BE, +40 RO, +41 fr-CH, +45 DK, and many more)

The following python script can be used to generate the DGA domain names. For Switzerland the seeds 1945 and 2931 are relevant:

```
#!/usr/bin/env python3

import argparse
import time
import math
from datetime import datetime

def get_seed(init, year, month):
    year = year
    month = month - 1
    j = ((year ^ month) ^ 0)
    j2 = j * 2
    j3 = j2 * (year ^ j2)
    j4 = j3 * (month ^ j3)
    # original java code uses long values which is limited to 64 bit
    j5 = (j4 * j4)%2**64
    seed = j5 + init;
    return seed


if __name__ == '__main__':
    parser = argparse.ArgumentParser(description = 'apk.flubot-dga')
    parser.add_argument('-s', '--seed', type=int, required = True)
    parser.add_argument('-y', '--year', help='default current year (YYYY)', type=int,
required = False)
    parser.add_argument('-m', '--month', help='default current month (MM)', type=int,
required = False)

    # parse arguments
    args = parser.parse_args()
    seedinit = args.seed
    now = datetime.utcnow()
    if args.year:
        year = args.year
    else:
        year = now.year
    if args.month:
        month = args.month
    else:
        month = now.month

    # generate domains
    domain = ""
    max_hosts = 5000
    seed = get_seed(seedinit, year, month)
    # class Random source, https://github.com/MostAwesomeDude/java-
random/blob/master/javarandom.py
    r = Random(seed)
    for i in range(max_hosts):
        label = ""
        for y in range(15):
            label = label + chr(r.nextInt(25) + 97);
        if (i % 3 == 0):
            domain = label + ".ru"
        elif (i % 2 == 0):
```

```
        domain = label + ".su";
    else:
        domain = label + ".cn";
    print(domain)
```

At the time of writing, the command and control server for the month of July for these two seeds are as following:

- Seed 1945, `dlnoryuolxttcvp.su`
- Seed 2931, `jaxubdocesmgxnb.su`

FluBot uses one of the following DNS lookup methods to resolve the DGA domain names:

- CloudFlare DNS Json API, `https://cloudflare-dns.com/dns-query?name=%s&type=A`
- Google DNS Json API, `https://dns.google/resolve?name=%s&type=A`
- Ali DNS Json API, `https://dns.alidns.com/resolve?name=%s&type=A`
- or classical DNS resolution over the network provisioned DNS resolver

A network operator who wants to block the communication to the c2 will not succeed by blocking DNS resolution to the c2 domain names as the malware can opt to use the other mentioned methods. However, in order to detect some infected mobile devices, it is useful and recommend to sinkhole infected bots and report the infection to the mobile user.

For all resolved domain names, FluBot uses public-/private crypto to communicate with the c2 server. Only if the c2 correctly answers the “ping” command of the bot it will attempt to register itself on the server. Sinkholing a c2 domain name does not allow to disrupt the communication but merely provides statistics of newly infected devices.

A FluBot DGA domain name typically resolves to up to 10 IP addresses. These IP addresses change within minutes or days. It will be hard for mobile operators to block all IP address in order to prevent FluBot from communicating with its c2 server. Even if the mobile operator were to succeed with that, most mobile devices will at some point enter a WiFi network where these defense mechanism are not in place. That said, it’s best to use network controls in order to detect infected devices and report these to the user.

Malware Capabilities

FluBot will upload the address book to the c2 server and then asks for an SMS rate at which it will send out smishing URLs to further infect other mobile phones. This is a worm like behavior. The typical SMS rate is between 10 and 30 seconds. At this rate, FluBot contacts its c2 server to receive SMS tasks. These tasks may look as following:

```
'0766430xxx,Neue Voicemail: https://taurus.dn.ua/voicemail/?cwidiwa'
'0763434xxx,Neue Voicemail: https://taurus.dn.ua/voicemail/?7l0mz7v9a7'
'0765430xxx,Neue Voicemail: http://swagtown420.com/y/?wgj3c3iov2'
'0766162xxx,Neue Voicemail: http://swagtown420.com/y/?q5eq4ii87c'
'0792869xxx,Neue Voicemail: https://lakonich.com/click/?07oqodq7'
'0764062xxx,Neue Voicemail: https://lakonich.com/click/?tla301m08o'
'0792159xxx,Neue Voicemail: http://rongnhosabudo.com/url/?8puv9uk2g4'
'0789228xxx,Neue Voicemail: http://rongnhosabudo.com/url/?6ljxntzuy'
'0754297xxx,Neue Voicemail: http://rongnhosabudo.com/url/?vg8edhyz'
'0793108xxx,Neue Voicemail: http://rongnhosabudo.com/url/?tgvv7adja'
'0794526xxx,Neue Voicemail: https://sazenlee.com/path/?hyzoatx'
```

This instructs the malware to send SMS to the given number with the shown text message.

The main malware capabilities are as follow:

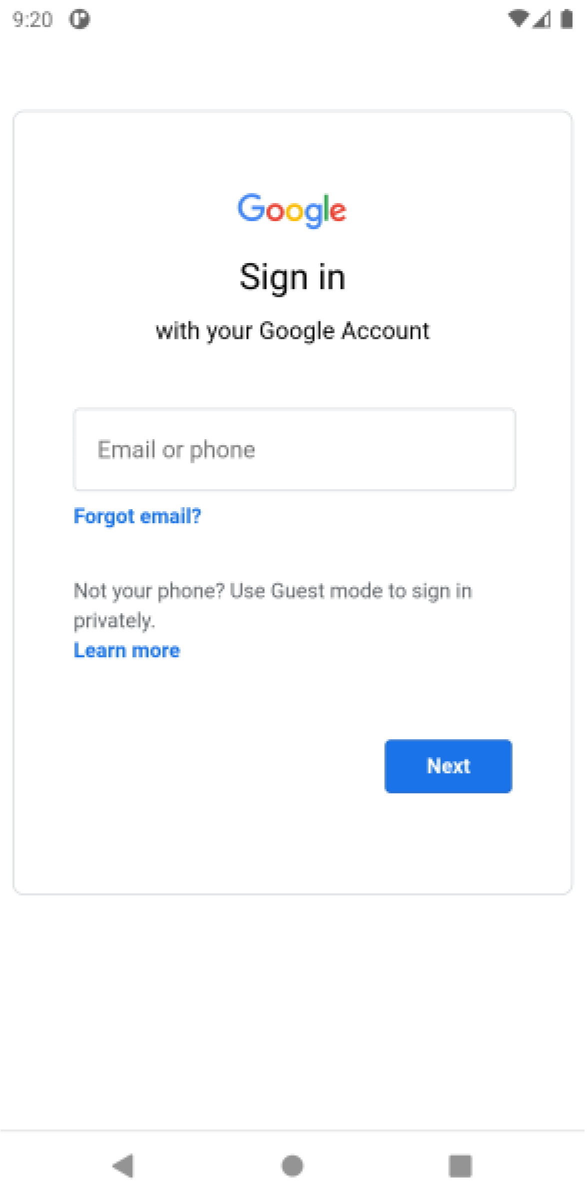
- read/block notifications
- read/block/send SMS messages
- steal contact list
- perform calls
- socks proxy (can be used by the fraudster to access the Internet)
- overlay for credential/cc phishing

For more detailed information about the capabilities, please refer to the linked technical reports in the section “Alias Names”.

The targeted apps for the overlay attack differ per country and also may change over time. At this time, the following apps are targetted by overlay attacks:

- Biance (Bitcoin), com.binance.dev
- Coinbase, com.coinbase.android
- Blockchain.com Wallet, piuk.blockchain.android
- Gmail, com.google.android.gm

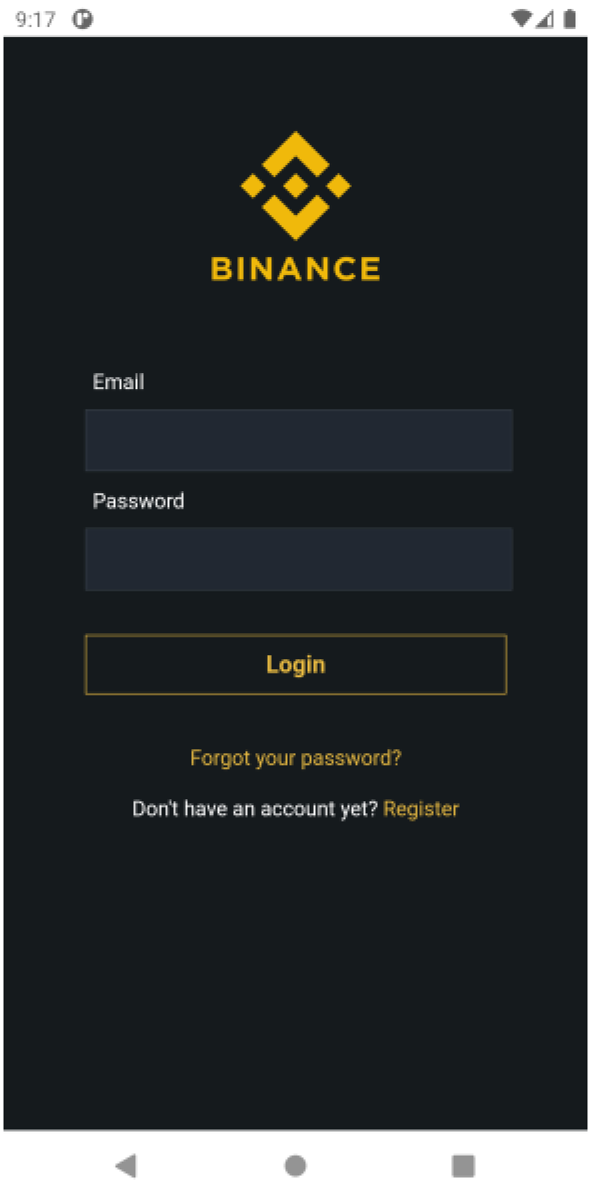
Following some example screenshots of the overlays for Gmail and Binance:



Sign in

with your Google Account

Not your phone? Use Guest mode to sign in privately.



Don't have an account yet? Register

IOCs

FluBot samples:

```
package name: com.baidu.searchbox
name: Voicemail
md5: b0989b77a305b7a542fd6e157d2380a2

package name: com.bilibili.app.in
name: Voicemail
md5: b0cd0ffb967b2c337c5850d07cd91159
```

Command and Control (c2) servers currently in use:

```
Seed 1945, dlnoryuolxttcvp.su
Seed 2931, jaxubdocesmgxnb.su
```

These c2 domain names are valid utmost until end of July 2021.