

# FluBot Malware Persists: Most Prevalent In Germany and Spain

 [bitsight.com/blog/flubot-malware-persists-most-prevalent-germany-and-spain](https://bitsight.com/blog/flubot-malware-persists-most-prevalent-germany-and-spain)

Written by André Tavares February 04, 2022 [Share Facebook](#) [Twitter](#) [LinkedIn](#)

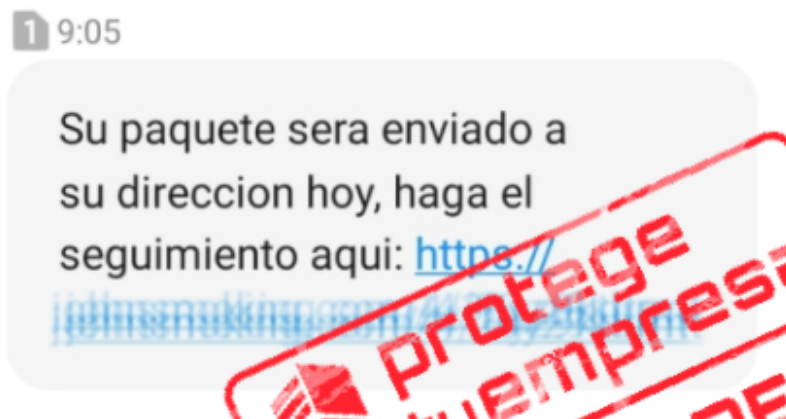
BitSight has been collecting FluBot infection telemetry data since March 2021. In total, we have identified 1.3 million IPs used by infected Android devices. Last month, it was mostly spread in Germany and Spain. Additionally, we are tracking an increase in IPs over time, which likely indicates an increase in infected devices.

First seen in early 2020, FluBot is a banking trojan used to steal banking, contact, SMS and other types of private data. Its operators have discovered creative means of distributing the malware, evolving their social engineering tactics and delivery methods to fuel the continued growth and expansion of FluBot.

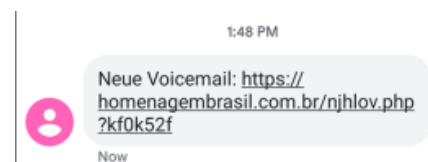
FluBot gives threat actors full remote control of an infected device, including the ability to send, intercept, and hide SMS messages and notifications; exfiltrate user sensitive data, such as contacts, keystrokes, one-time passcodes, and personal information; and carry out overlay attacks.

The malware is commonly spread via SMS messages to the contacts on an infected device as well as contacts downloaded from FluBot's C2 server. FluBot typically appears as a message for package delivery. Below are some examples:


## Malicious SMS Messages




(source: [incibe.es](https://incibe.es))



(source: [switch.ch](https://switch.ch))



## Seguimiento de su paquete



**Descargar la aplicación**

1. Este paquete está vinculado a su número de teléfono y sólo puede ser rastreado con nuestra aplicación.
2. Si aparece una ventana que impide la instalación, seleccione "ajustes" y active la instalación de aplicaciones desconocidas.

(source: [incibe.es](http://incibe.es))

patukiposhak.com.au/voice

**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.

[Voicemail-App herunterladen](#)

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

(source: [switch.ch](http://switch.ch))

**Report: 3 out of 4 mobile applications evaluated contained at least one Moderate vulnerability**



## Report: 3 out of 4 mobile applications evaluated contained at least one Moderate vulnerability

---

Get BitSight's latest research on mobile application security where you'll find eye-opening statistics on the state of mobile application security today, examples of how and why mobile breaches occur, and actionable advice for mitigating risks associated with your own mobile applications, as well as apps from third-party partners and suppliers.

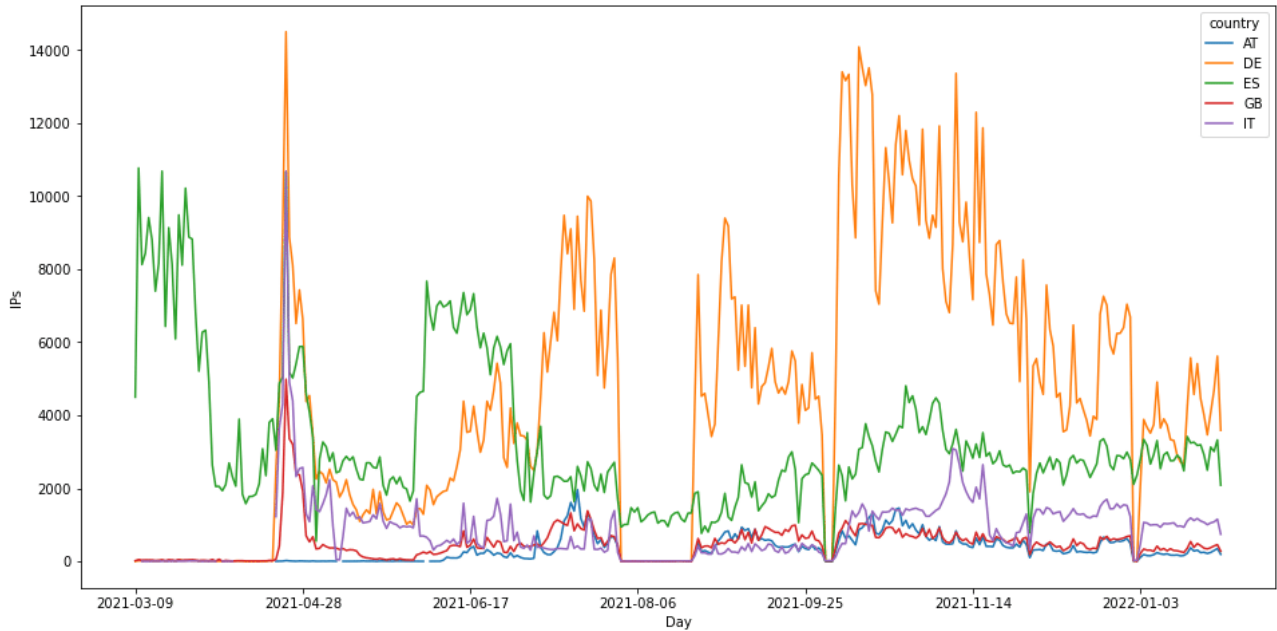
[Download Report](#)  
[Button Arrow](#)

### BitSight's Observations

---

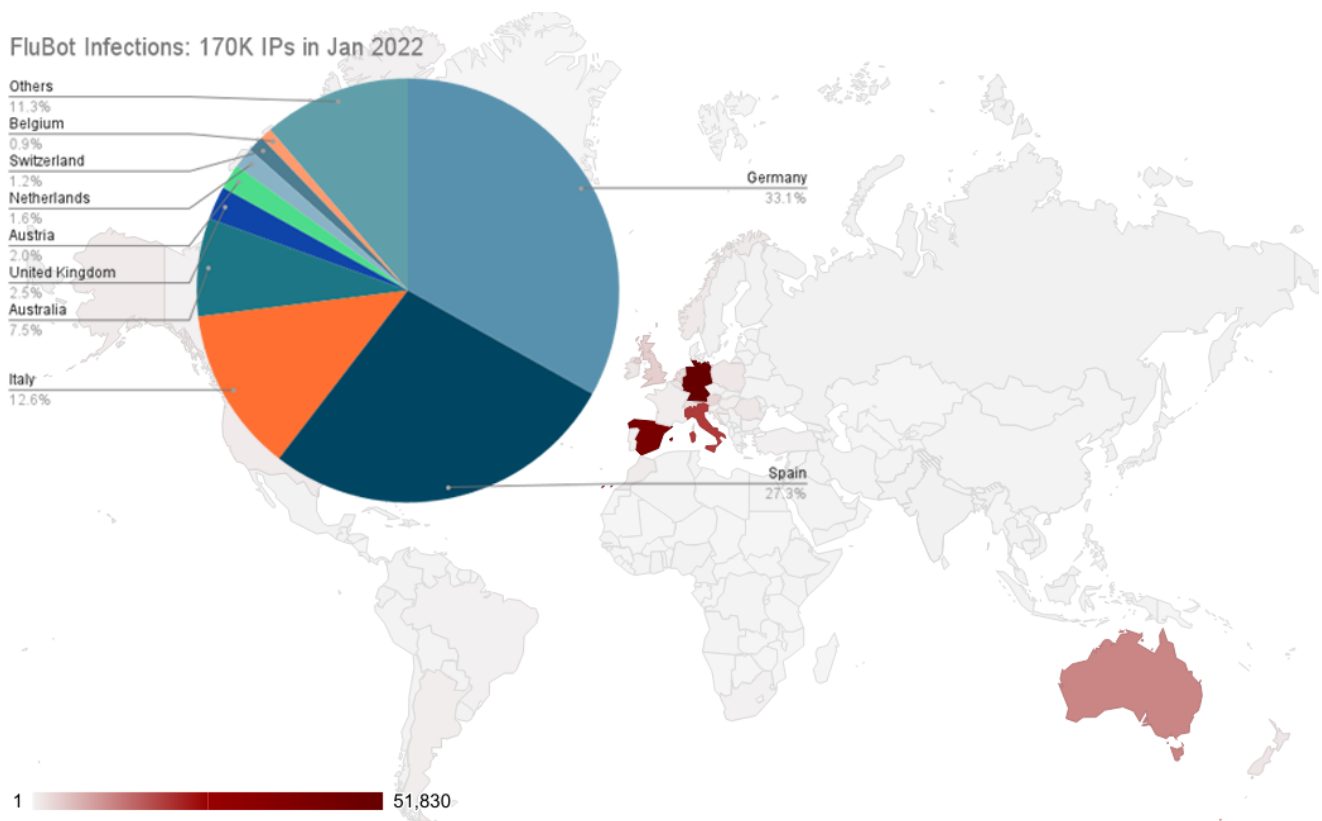
BitSight currently observes FluBot is mostly spread in Europe, specifically in Germany, Spain and Italy (74%), but also in Australia (7%). This appears to track with recent reports that suggest Flubot operators specifically target different regions or countries. However, it may also be a function of how FluBot spreads. It stands to reason that the majority of a victim's contacts are people in the same region or country. So, regional infection may not be intentional per se, but rather a consequence of the malware's design.

Below is a chart showing daily FluBot infections by country that BitSight has detected since March 2021, highlighting the consistent impact to German and Spanish users.



Since BitSight began tracking FluBot, we have also seen an increase of impacted IPs. The number of IPs does not directly correspond to the number of infected devices, because a mobile device can share the same IPv4 address as other devices due to network address translation (NAT) and IPv4 exhaustion. However, a rise in IPs may be an indicator of rising device infections.

The following diagrams show our visibility into the geographical distribution of all FluBot versions in January 2022.



In January, approximately 170,000 IPs (used by infected devices) contacted our sinkhole infrastructure. The majority of those are infected with FluBot versions 4.8 and earlier. These versions communicate with its C2 server via HTTPS. Since version 4.9, FluBot has communicated with its C2 server via DNS-Tunneling-over-HTTPS (DoH). Of the 170,000 IPs observed in January, approximately 30,000 were infected with FluBot 4.9 through 5.2 (the current version at the time of this writing).

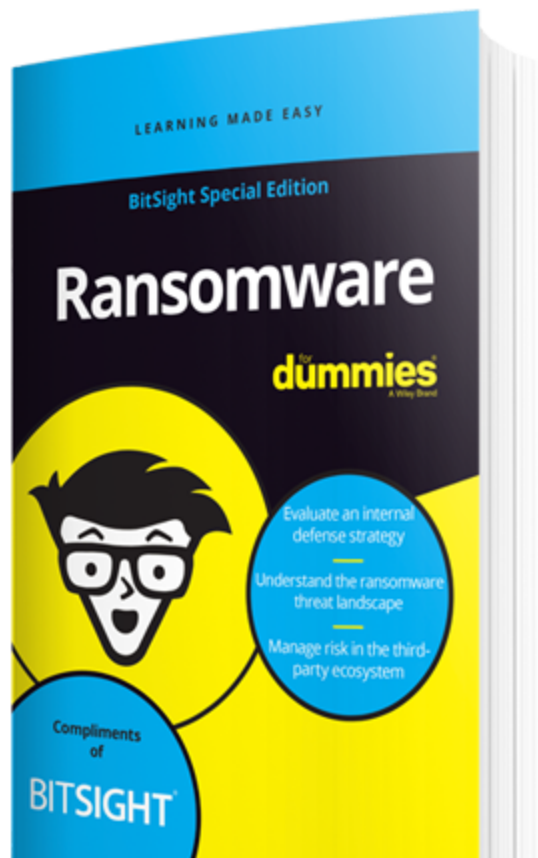
FluBot uses a domain generation algorithm (DGA) to be able to communicate with its C2 server. On version 5.1, there was an update on the DGA (python version on the IOCs section). Changes include a new additional seed that is downloaded from the C2 server to generate more domains.

## BitSight Exclusive: Ransomware for Dummies

---

Bring your strategic defense to the next level

---



## BitSight Exclusive: Ransomware for Dummies

---

Bring your strategic defense to the next level

---

Ransomware attacks globally nearly doubled in 2021. BitSight's Ransomware for Dummies book reveals indicators of potential attacks, and how to minimize costly damage when successful ransomware targets you.

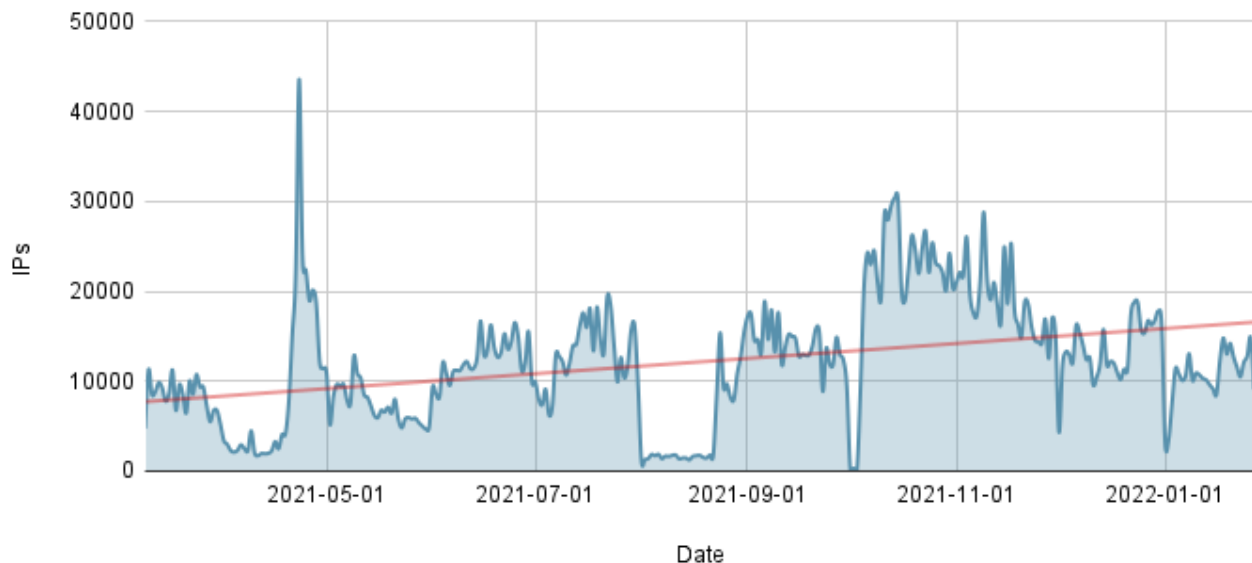
[Download eBook](#)

[Button Arrow](#)

Using these newer versions, an attacker sets a nameserver that will act as a C2 server, receiving and sending data through the DNS protocol; FluBot uses DoH providers such as Google and Cloudflare to infiltrate and exfiltrate the data to the C2 server, allowing the infected device to communicate with its C2 server without knowing its IP address.

The DNS provider routes the DNS request to the C2 server (nameserver), which returns a TXT DNS response as requested by the bot. The request contains a symmetric key generated by the bot that is RSA encrypted, and the private key is on the C2 server side.

### FluBot infections: 1.3M IPs



Note: The drop reflected in August is due to temporary collection issues.

## Mitigating FluBot

While FluBot operators do not appear to be specifically targeting organizations as opposed to individuals, it is still critical for security professionals to take appropriate steps to mitigate risk.

Since FluBot is spread using social engineering, employee education is essential. Share examples of FluBot SMS messages and malicious lure pages so employees know what to look for. Effective employee training can avert FluBot infection entirely.

Anti-malware software should be considered essential to prevent, detect, and remove FluBot infections. FluBot can be removed manually, however, manual removal may be time-consuming—especially if the infection is widespread. Mobile device management (MDM) solutions that can restrict the ability to install apps may be appropriate for some organizations, as well.

BitSight has identified a number of indicators of compromise (IOC), which are detailed below:

### **FluBot samples (APKs)**

---

df98a8b9f15f4c70505d7c8e0c74b12ea708c084fbbffd5c38424481ae37976f  
29d71a81bb8aa363d93adc9352e791720263935fb4c9cc0cfc20be0d1c6d3fdc  
8ef32886de7fb2fcfbde483044ef21a196ea5525df04e0f391ef491b62959de1  
5b404c066e702802b7475d2c2eecebd6fceb2490773f92d501d57b53de34213c  
4859ab9cd5efbe0d4f63799126110d744a42eff057fa22ff1bd11cb59b49608c  
dcb5e9c2f2c7c2a94b6419527361790132af20d60e681ca87c0c5257393cbac8  
4a49972ed962b5326b9edcb9edbfeef47d3a216cf5847d579eb0c69a3ed6b9be  
d1e40e321456c2a9e6d06c4e79961d388cd55050c055f47cdd9e0a2db571916b  
af83e659196774e779b22038e11c4b0a4665d082064fe997510634000fdb0222  
a2d3292bb87f8d6b3ce4b45d9ae6d61b4b7398770f732b72c881f43b66a49461

### **FluBot DGA v3 implemented in Python**

---

```

import argparse
from datetime import datetime
# https://github.com/MostAwesomeDude/java-random/blob/master/javarandom.py
from javarandom import Random

def get_seed(init, year, month):
    month = month - 1
    j = ((year ^ month) ^ 0)
    j2 = j * 2
    j3 = j2 * (year ^ j2)
    j4 = j3 * (month ^ j3)
    j5 = (j4 * j4) % 2 ** 64
    seed = j5 + init
    return seed

if __name__ == '__main__':
    parser = argparse.ArgumentParser(description='FluBot DGA v3')
    parser.add_argument(
        '-s', '--seed', choices=[1949, 1945, 1813, 1136, 2931, 1642, 1905], 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

    r = Random(seed=get_seed(seedinit, year, month))
    tlds = ['ru', 'cn', 'com', 'org',
            'pw', 'net', 'bar', 'host',
            'online', 'space', 'site',
            'xyz', 'website', 'shop',
            'kz', 'md', 'tj', 'pw', 'gdn',
            'am', 'com.ua', 'news', 'email',
            'icu', 'biz', 'kim', 'work',
            'top', 'info', 'br']

    for i in range(2500):
        domain = ''
        for _ in range(15):
            domain += chr(r.nextInt(25) + 97)

```



```
domain = f'{domain}.{tlds[i % len(tlds)]}'  
print(domain)
```

## Get A Free Attack Surface Report

---



## Get A Free Attack Surface Report

---

Request your free custom report and see how you can start reducing your cyber risk exposure across your digital ecosystem: cloud assets across all geos & subsidiaries; discover shadow IT; security risk findings; and more!

[Get Your Report](#)  
[Button Arrow](#)

## Get the Weekly Cybersecurity Newsletter

---

Subscribe to get security news and industry ratings updates in your inbox.

•

- \*

[Read more](#)

By checking this box, I consent to sharing this information with BitSight Technologies, Inc. to receive email and phone communications for sales and marketing purposes as described in our [privacy\\_policy](#). I understand I may unsubscribe at any time.