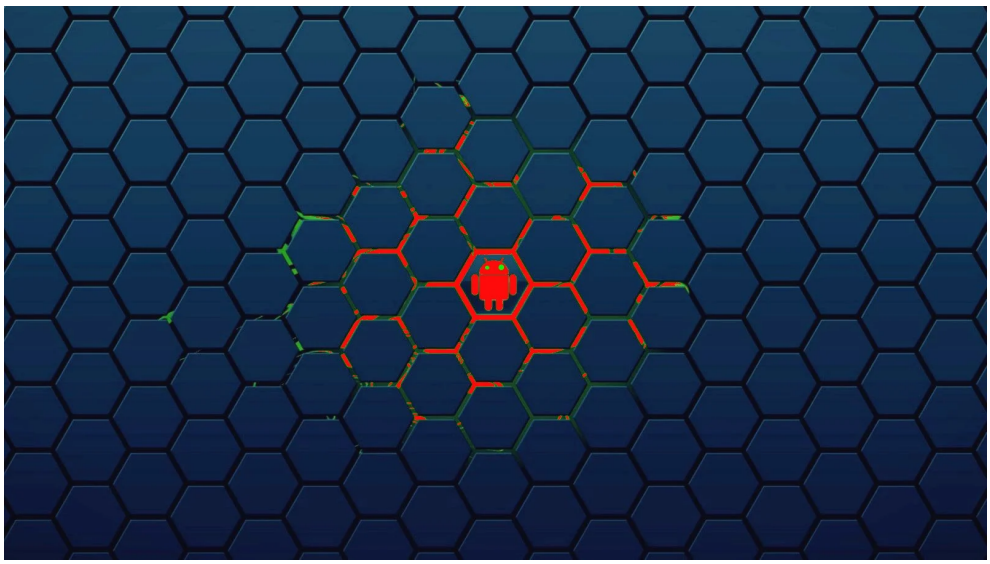
FluBot malware now targets Europe posing as Flash Player app

By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)** January 7, 2022 12:37 PM **0**



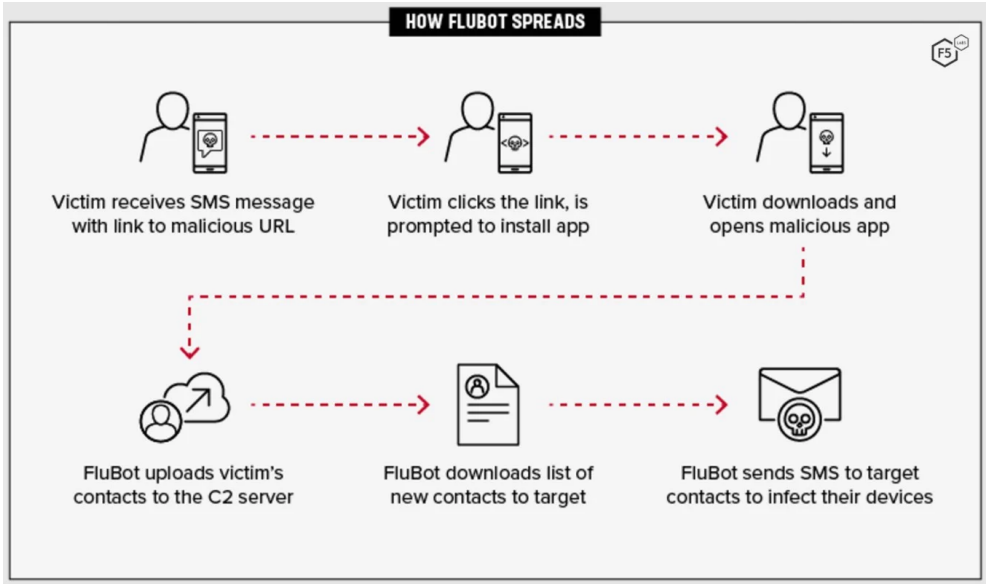
The widely distributed FluBot malware continues to evolve, with new campaigns distributing the malware as Flash Player and the developers adding new features.

FluBot is an Android banking trojan that steals credentials by displaying overlay login forms against many banks worldwide.

The smishing (SMS phishing) lures for its distribution include fake security updates (https://www.bleepingcomputer.com/news/security/flubot-android-malware-now-spreads-via-fake-security-updates/), fake Adobe Flash Players (https://twitter.com/malwrhunterteam/status/1478099419392319493), voicemail memos (https://www.bleepingcomputer.com/news/security/finland-warns-of-flubot-malware-heavily-targeting-android-users/), and impersonating parcel delivery notices.

Once in the device, FluBot can steal online banking credentials, send or intercept SMS messages (and one-time passwords), and capture screenshots.

Because the malware uses the victim's device to send new smishing messages to all their contacts, it usually spreads like wildfire.



FluBot spread process diagram

Source: F5 Labs

Impersonating Flash Player

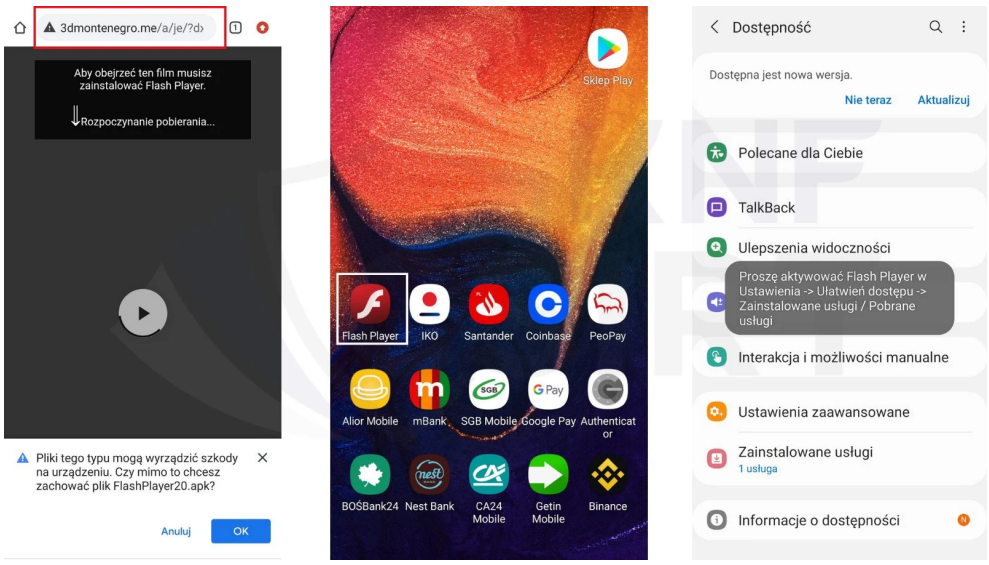
MalwareHunterTeam told BleepingComputer that new FluBot campaigns are distributed using SMS texts asking the recipient if they intended to upload a video from their device.

An example of this campaign's SMS text targeting Polish recipients was shared by CSIRT KNF (https://twitter.com/CSIRT_KNF/status/1478008084673011714), as seen below.

FluBot SMS text asking if the user uploaded a video

Source: CSIRT KNF

When recipients click on the included link, they are brought to a page offering a fake Flash Player APK [VirusTotal (https://www.virustotal.com/gui/file/e68896724122adbfcc44955cdd688aa9e153687d1b804d812cb1f3332a9e9bcd)] that installs the FluBot malware on the Android device.



FluBot fake Flash Player attack chain

Source: CSIRT KNF

Android users should always avoid installing apps from APKs hosted at remote sites to protect themselves from malware. This practice is especially true for well-known brands, like Adobe, whose apps should only be installed from trusted locations.

New features in recent FluBot versions

The most recent major release is version 5.0, which came out in early December 2021, while version 5.2 saw the light only a few days ago.

With this release, the DGA (domain generation algorithm) system received much attention from the malware authors, as it's vital in enabling the actors to operate unobstructed.

DGA generates many new C2 domains on the fly, making mitigation measures such as DNS blocklists ineffective.

In its newest version, FluBot's DGA uses 30 top-level domains instead of just three used previously and also features a command that enables attackers to change the seed remotely.

```
DGA.generate_seed_by_date();
AtomicReference hostRef = new AtomicReference();
hostRef.set(null);
Random r = new Random(DGA.seed);
SharedPreferences prefs = pc60bc747.b().getSharedPreferences(pc60bc747.b().getString(0x7F0F001C), 0);
String priorityHost = prefs.getString("f", null);
ArrayList hostList = new ArrayList();
int i = 0;
int tldC;
for(tldC = 0; i < 5000; ++tldC) {
    String host2test = "";
    int y;
    for(y = 0; y < 15; ++y) {
        host2test = host2test + ((char)(r.nextInt(25) + 97));
    }

    String[] v9_1 = DGA.tld_list;
    if(tldC >= v9_1.length) {
        tldC = 0;
    }

    hostList.add(host2test + v9_1[tldC]);
    if(i > 0 && i % 20 == 0 && priorityHost != null) {
        hostList.add(priorityHost);
    }

    if(i == 2500) {
        long altSeed = prefs.getLong("g", 0L);
        if(altSeed == 0L) {
            break;
        }

        r = new Random(altSeed);
    }

    ++i;
}
```

Function responsible for domain generation

Source: F5 Labs

On the communication side, the new FluBot now connects to the C2 through DNS tunneling over HTTPS, whereas previously, it used direct HTTPS port 443.

The commands added on the malware in versions 5.0, 5.1, and 5.2, are the following:

- Update DNS resolvers
- Update the DGA seed remotely
- Send longer SMS messages using multi-part division functions

Along with the above, the latest version of FluBot retains the capability to:

- Open URLs on demand
- Get the victim's contact list
- Uninstall existing apps
- Disable Android Battery Optimization
- Abuse Android Accessibility Service for screen grabbing and keylogging
- Perform calls on demand
- Disable Play Protect
- Intercept and hide new SMS messages for stealing OTPs
- Upload SMS with victim information to C2

- Get list of apps to load the corresponding overlay injects

In summary, FluBot hasn't deprecated any commands used in previous versions and only enriched its capabilities with new ones.

For more technical details on how exactly the latest version of FluBot works, check out the F5 Labs report (https://www.f5.com/labs/articles/threat-intelligence/flubots-authors-employ-creative-and-sophisticated-techniques-to-achieve-their-goals-in-version-50-and-beyond).

How to stay safe from FluBot

Note that in many cases, a link to download FluBot will arrive on your device via one of your contacts, maybe even a friend or family.

As such, if you receive an unusual SMS that contains a URL and urges you to click it, it's likely a message generated by FluBot.

Finally, avoid installing APK files from unusual sources, regularly check that Google Play Protect is enabled on your Android device, and use a mobile security solution from a reputable vendor.

Related Articles:

Flubot Android malware now spreads via fake security updates (https://www.bleepingcomputer.com/news/security/flubot-android-malware-now-spreads-via-fake-security-updates/)

Android banking trojan spreads via fake Google Play Store page (https://www.bleepingcomputer.com/news/security/android-banking-trojan-spreads-via-fake-google-play-store-page/)

Anubis Android malware returns to target 394 financial apps (https://www.bleepingcomputer.com/news/security/anubis-android-malware-returns-to-target-394-financial-apps/)

Android banking malware infects 300,000 Google Play users (https://www.bleepingcomputer.com/news/security/android-banking-malware-infects-300-000-google-play-users/)

Malicious Android app steals Malaysian bank credentials, MFA codes (https://www.bleepingcomputer.com/news/security/malicious-android-app-steals-malaysian-bank-credentials-mfa-codes/)