FluBot Android Zararlı Yazılım Analizi

infinitumit.com.tr/flubot-zararlisi/

infinitumit 16 Ağustos 2022

FluBot Analiz Özeti

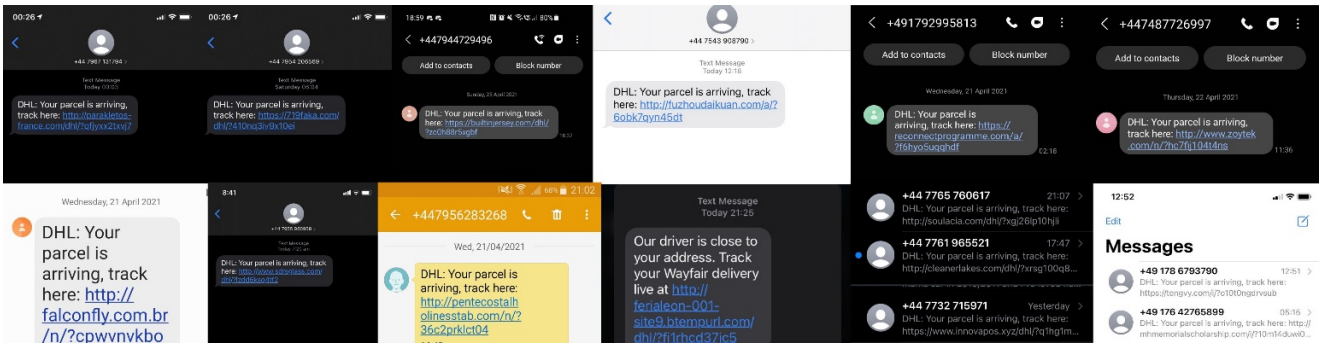
FluBot zararlısı Android cihazları hedefleyen ve sahte SMS'ler aracılığıyla kurbanlara enjekte edilen bir zararlı yazılımdır. Oltalama (phishing) yöntemleri kullanılarak hazırlanan sahte SMS FluBot'un indirilmesini sağlayan bağlantıyı içerir. Bu bağlantıya tıklayan kurbanlar .apk uzantılı bir dosya indirirler. Kurulum işleminden sonra FluBot zararlısı komuta kontrol (C2) sunucusu ile iletişim kurarak cihazı uzaktan yönlendirir.

Gerçekleştirilen analizler sonucunda FluBot zararlısının kurban cihaz üzerinden SMS gönderme, gelen kısa mesajları okuma, arka plan uygulamalarını kapatma ve telefon rehberine erişme gibi yeteneklere sahip olduğu tespit edilmiştir.

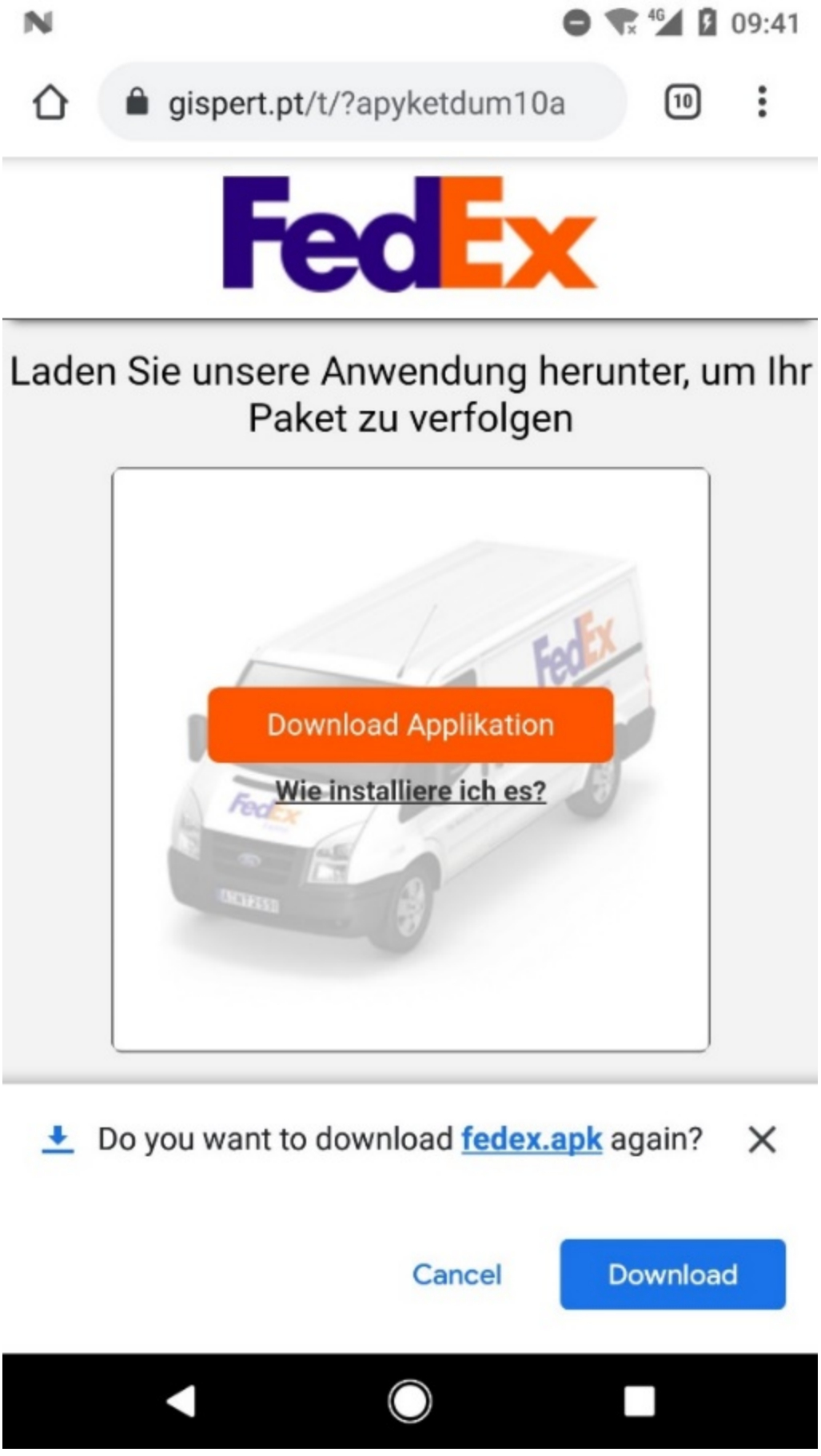
Kurulum sonrası zararlı gerekli izinleri kurbandan aldıktan sonra ilgili oltalama senaryosu gereği kurbanı bir forma yönlendirir. Bu sayfada kurbandan doğum tarihi, ad-soyad, kredi kartı bilgisi ve telefon numarası gibi hassas bilgiler temin edilir. Ardından temin edilen bilgiler

FluBot aracılığıyla saldırgana ait komuta kontrol sunucusuna gönderilir.

Sahte DHL SMS bilgilendirme mesajı (Phishing)

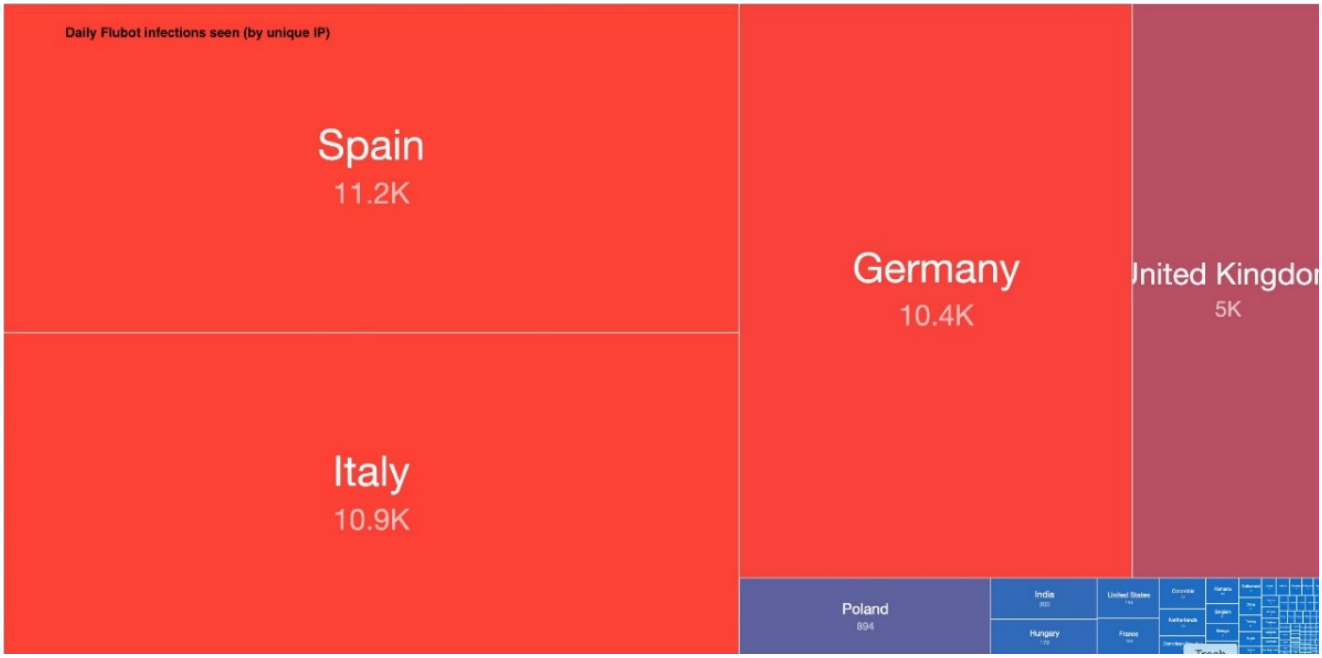


Başka bir örnekte ise FluBot'un sahe SMS ile kurban sisteme yüklenmesi işlemi göze çarpıyor. Hedef kullanıcı SMS ile gelen linke tıkladıktan sonra gelen web sayfası üzerinde, zararlı yazılımı indirmesi için hazırlanan sahte ve gerçekçi bir sayfa ile karşılaşıyor. (Örnek oltalama sayfasına ilişkin ekran görüntüsü aşağıda şekilde yer almaktadır)


09:41
gispert.pt/t/?apyketdum10a
10
FedEx
Laden Sie unsere Anwendung herunter, um Ihr Paket zu verfolgen
Download Applikation
Wie installiere ich es?
Do you want to download fedex.apk again?
Cancel
Download

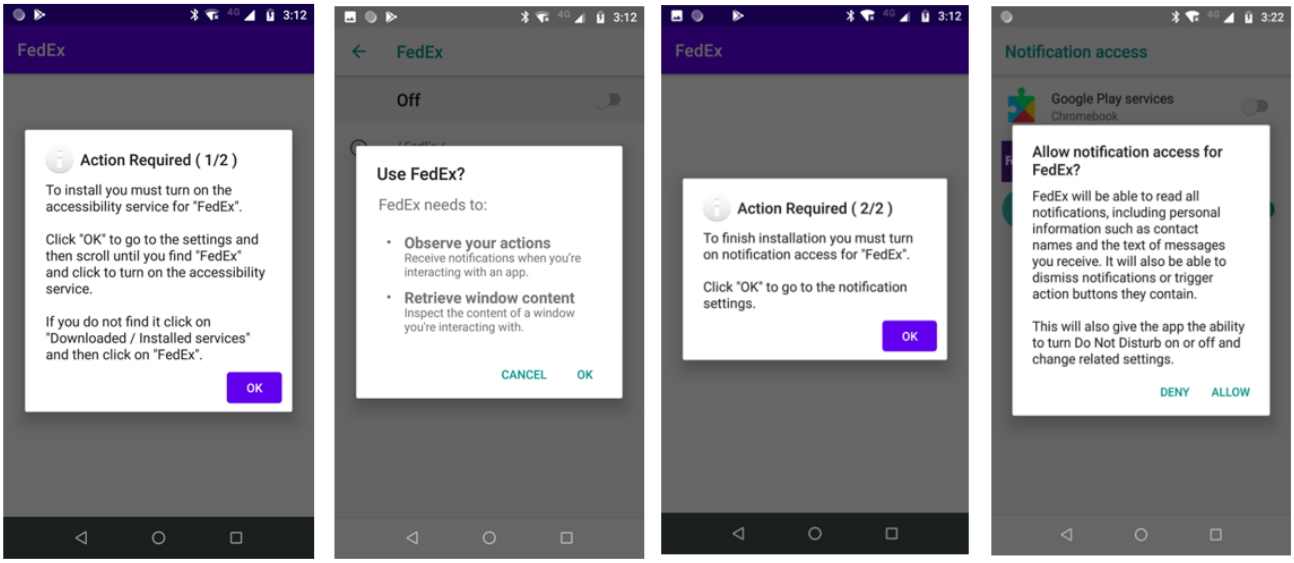
Bulaşma Sıklığı ve Hedef Ülkeler

FluBot zararlısı yoğunluklu olarak ile Avrupa ülkelerini hedef seçmiştir. COVID sonrası artan paket dağıtım hizmetlerini phishing aracı olarak kötüye kullanmıştır böylece kısa bir zaman içinde çok hızlı bir yayılmaya sahip olmuştur.



FluBot Teknik Analizi

FluBot zararlısı indirildikten sonra cihaz içinde “full access” yetkisi verilmesi için kullanıcı onayı istemektedir. Onay, hedef kullanıcı tarafından verildikten sonra hedef kullanıcı uygulamayı kapatsa bile zararlı yazılım arka planda çalışmaya devam etmektedir.



Arka planda çalışan “com.eg.android.AlipayGphone” (FluBot) zararlısına ait izin listesi şu şekildedir:

- android.permission.INTERNET
- android.permission.READ_CONTACTS
- android.permission.WRITE_SMS
- android.permission.READ_SMS
- android.permission.SEND_SMS
- android.permission.RECEIVE_SMS
- android.permission.READ_PHONE_STATE
- android.permission.QUERY_ALL_PACKAGES
- android.permission.WAKE_LOCK
- android.permission.FOREGROUND_SERVICE
- android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
- android.permission.CALL_PHONE
- android.permission.REQUEST_DELETE_PACKAGES
- android.permission.KILL_BACKGROUND_PROCESSES
- android.permission.ACCESS_NETWORK_STATE

Yukarıdaki izinlerle erişen, kötü amaçlı yazılım aşağıdaki eylemleri gerçekleştirebilir hale gelmektedir.

• İnternet erişimi

• SMS Okuma / Gönderme

• Telefon rehberini okumak

• Çağrı Yapma

• Cihaz içinden uygulama silme

• Erişilebilirlik hizmetini kullanma yeteneği

• Cihaz bildirimlerini okuma

Hedef kullanıcıya ait Android cihaz artık sürekli olarak saldırganlara ait komuta kontrol sunucusu ile iletişim halindendir. Analizlerimiz sonucunda bu iletişimin saldırganın isteğine göre SOCKS Proxy üzerinden devam edebildiği tespit edilmiştir.

```
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;
        }
```

3.1- String Obfuscation (Karmaşıklaştırma)

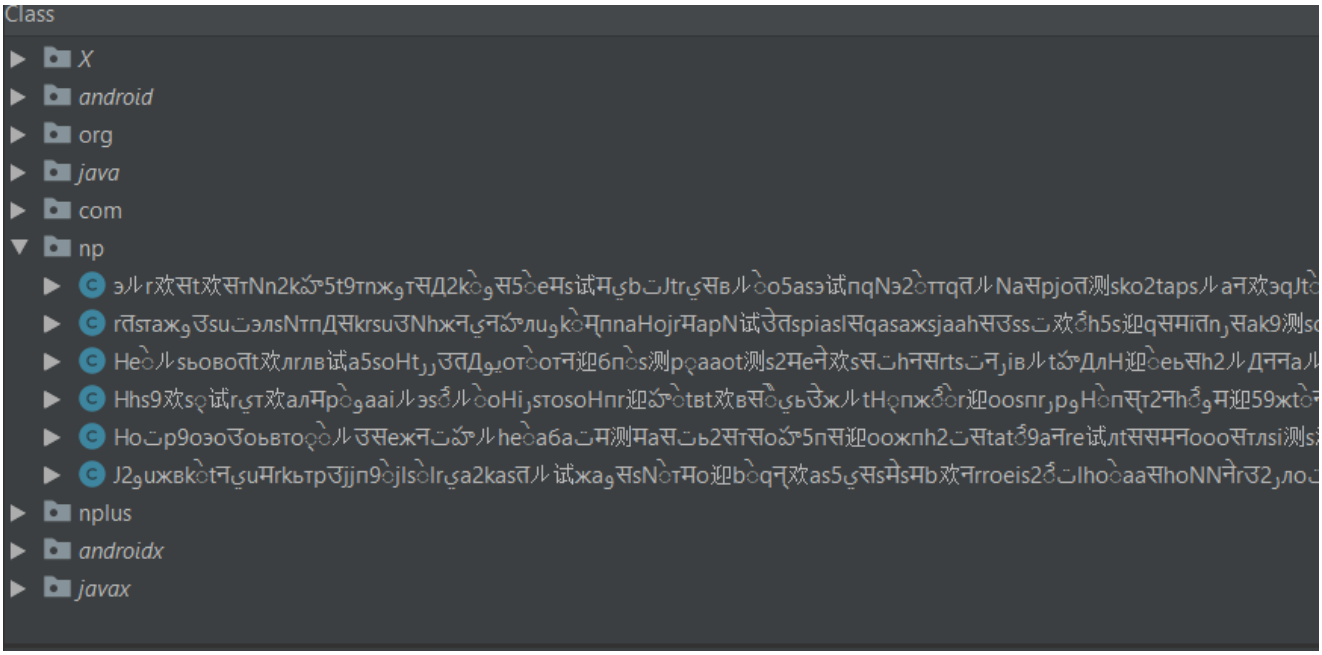
FluBot zararlısı incelemeyi zorlaştırmak ve anti virüs yazılımlarını bypass etmek (atlatmak) için açık kaynak kodlu olan Paranoid isimli String obfuscator yazılımını kullanır böylece zararlı yazılıma çalışma aşamasında String verilerini gizleme özelliği kazandırılır.

Obfuscate edilen String veriler:

• BotId

• BrowserActivity

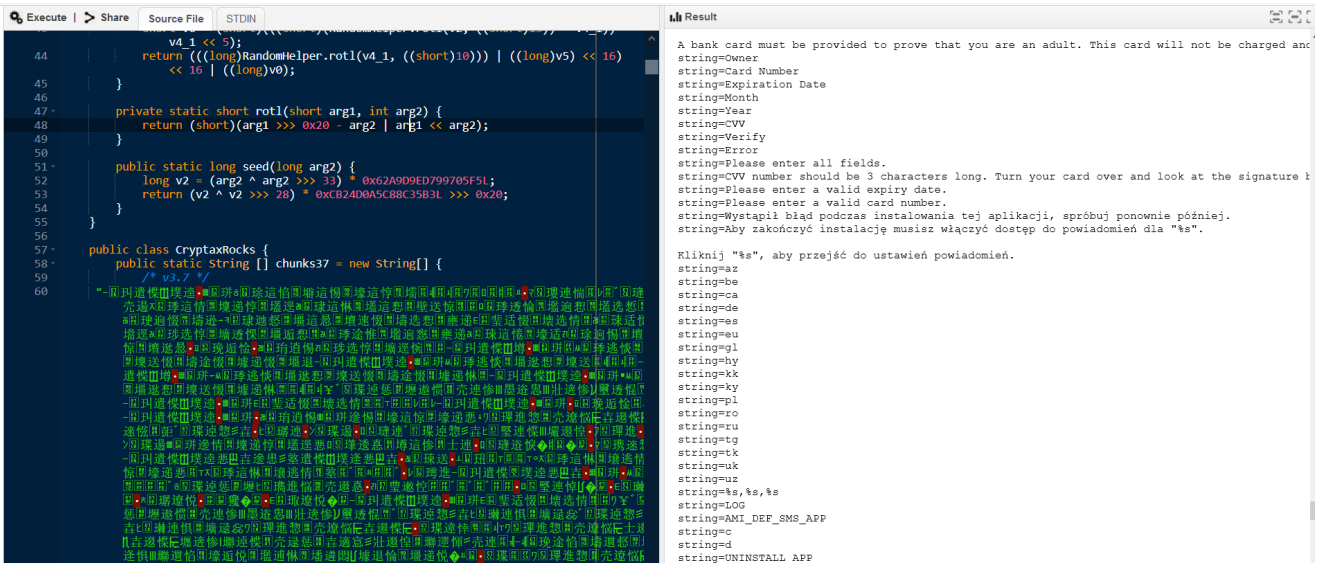
- CardActivity
- ComposeSmsActivity
- ContactItem
- DGA
- ForegroundService
- HttpCom
- IntentStarter
- LangTxt
- MainActivity
- MyAccessibilityService
- MyNotificationListener
- PanelReq
- SmsReceiver
- Spammer
- Utils
- SocksClient
- PanelReq



3.2 – String De-obfuscate

FluBot zararlısına ait String veriler saldırganlar tarafından gizlenir, analiz sonuçlarının doğrulu için Obfuscated olan String verilerim De-obfuscate edilmesi gerekmektedir. Bu işlem için açık kaynak kodlu olan bir Java yazılımından yararlanılmıştır.

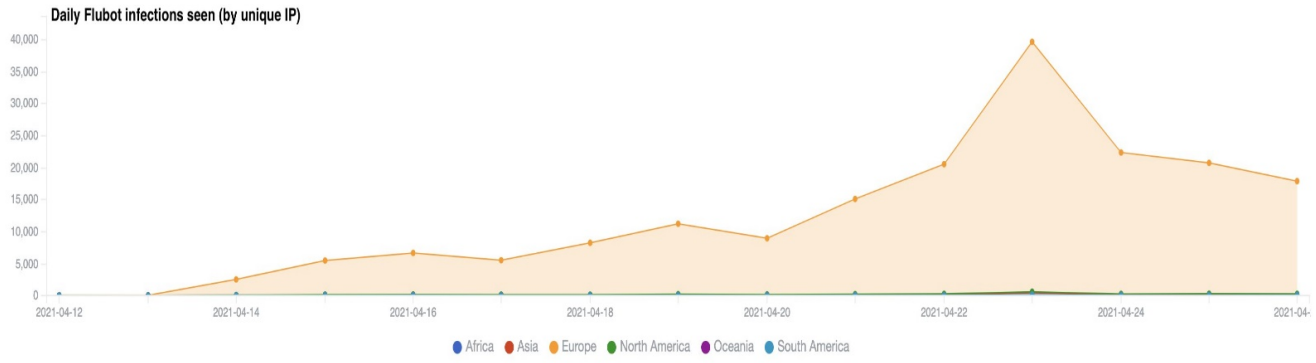
Java yazılımı çalıştırıldığında chunks37 dizisi içerisinde bulunan veri matematiksel bir fonksiyon ile anlaşılır String veriye dönüştürülür. Sağ kısımda görüldüğü gibi çıktı olarak üretilen veri içerisinde farklı dillere ait phishing aşamasında kullanılan String veriler mevcuttur. (Card Number, CVV, Owner,Year vb.)



3.3 – Command And Control (Komuta Kontrol)

FluBot zararlısına ait en yeni versiyon 4.0 olarak ortaya çıkmıştır. FluBot hedef Android cihaza girdikten sonra saldırgan ile bağlantı kurmak için **Domain Generation Algorithm (DGA)** isimli bir algoritma yardımı ile random sayı ve harflerden oluşan bir domain oluşturmakta ve böylece saldırganlara ait komuta kontrol sunucuları bot yazılımlardan gizlenebilmektedir. Bağlantı özellikle 4.0 versiyonunda DNS veya DNS over HTTPS şeklinde gerçekleşmektedir. Böylece zararlı yazılım hedef cihaza bağlantı istek paketleri gönderdiği zaman güvenlik duvarı , EDR veya Anti Virüs sistemlerinden kaçınmaktadır.

2021-01-22 tarihinde başlayan yükseliş 4.0 versiyonu ile gerçekleşmiştir.



Google DNS özelliği saldırganlar tarafından kötüye kullanılmış böylece Google DNS tünel olarak kullanılıp saldırgana ait **Command and Control** sunucularına DNS üzerinden bağlantı istekleri yapılmaktadır. HTTP isteklerine ilişkin ekran görüntüsü aşağıda yer almaktadır.

HTTP Requests

+ https://dns.google:443/resolve?name=xpbftfjvnxnvwhj.cn&type=A
+ https://dns.google:443/resolve?name=mfdkmrmsklrkpqd.cn&type=A
+ https://dns.google:443/resolve?name=vgckubmcmolbihn.su&type=A
+ https://dns.google:443/resolve?name=gmpyorbwiawwrlw.cn&type=A
+ https://dns.google:443/resolve?name=hvlpydfmdxshnff.su&type=A
+ https://dns.google:443/resolve?name=vrrssctjuvtbceb.su&type=A
+ https://dns.google:443/resolve?name=vcyfeejpddeqhct.cn&type=A
+ https://dns.google:443/resolve?name=rqnoeeclnomhbbu.cn&type=A
+ https://dns.google:443/resolve?name=pfqavwbcvokinfe.su&type=A
+ https://dns.google:443/resolve?name=blefyvouieeleyb.su&type=A

DGA ile oluşturulan Command And Control sunucuları:

DNS Resolutions

+ nndivlkgwghxpqr.su
+ oqgqoyqpnhrimst.ru
+ dkysaurdvwbjdtm.ru
+ egukjpirniyuifp.su
+ lngibrgfwhslqum.su
+ qlbkawvceyvpteb.su
+ trasxtamqinibym.ru
+ fydnuvsfjlukaew.cn
+ qggbjbawevnjppk.cn
+ teptxcfqelemxkw.ru

FluBot 4.0 versiyona ait “**poll.php**” üzerinden yapılan bağlantı isteğini gerçekleştiren fonksiyon, saldırgan C2 sunucusu üzerinden (PING,LOG,SMS_RATE,GET_SMS vb.) komutlarını uzaktan çalıştırabilmektedir.

```
    method.static.constructor.Lcom_eg_android_AlipayGphone_k.Lcom_eg_android_AlipayGphone_k.method.
    _clinit___V
              (void)

{
  undefined4 puVar1;
  undefined4[] ppuVar2;

                    /* 4.0 */
  a.a(-0x330cf826b942);
                    /* /poll.php */
  a.a(-0x3310f826b942);
                    /* a */
  a.a(-0x331af826b942);
                    /* b */
  a.a(-0x331cf826b942);
                    /* c */
  a.a(-0x331ef826b942);
                    /* d */
  a.a(-0x3320f826b942);
                    /* e */
  a.a(-0x3322f826b942);
                    /* f */
  a.a(-0x3324f826b942);
                    /*
                    MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAiQ3YWOM6ycmMrUGB8b3LqUiuXdxFYm/eBxAR
                    oAHC/9dC8c6agwdveSqj3/9hTOM5zTS/OsrYlIT6+ZmmmZrnOfbB+FXq3pCG8/kM6ujvGxY0ANfbGVlf
                    CTOnd+jKVHH1YhPT55aAY5K0C0EACXoV+TyyjReAtzC2xn4gI/tklOOfK2/17qaOIuYLneGHRuklmM/B
                    VMvlg9st4If6WYyntcX6RZtY7Usks7MWVhFOpzYlLN02b/FAPWjbgOPehZUqz8WGAuHFjuAX99c65nsY
                    m1UT9IYypQXx3KJMBeJr1Yr4VUkkPMRqgAbKacWvgDywkJuYOcbfz8Om8a+8TVaojwIDAQAB
                       */
  a.a(-0x3326f826b942);
                    /* PREPING */
  a.a(-0x34aff826b942);
                    /* PING */
  a.a(-0x34b7f826b942);
                    /* LOG */
  a.a(-0x34bcf826b942);
                    /* SMS_RATE */
  a.a(-0x34c0f826b942);
                    /* GET_SMS */
  a.a(-0x34c9f826b942);
                    /* GET_INJECT */
  a.a(-0x34d1f826b942);
                    /* GET_INJECTS_LIST */
  a.a(-0x34dcf826b942);
                    /* CONTACTS */
  a.a(-0x34edf826b942);
```

Analizlerimiz sonucunda ortaya çıkan, FluBot zararlısının hedef cihaza uzaktan erişmek için DNS over HTTPS bağlantısını sağlamak ile görevli decompile edilmiş fonksiyon aşşağıda yer almaktadır.

Bu saldırı yöntemi özellikle İngiltere ve Amerika'da bulunan hedefler için seçilmiştir. En önemli fark ise FluBot 4.0 zararlısına ait farklı bir örnekte saldırganların bağlantı almak için Google DNS yerine Cloudflare DNS'i seçmiş olmalıdır.

```
method.static.public.Lcom_eg_android_AlipayGphone_n.Lcom_eg_android_AlipayGphone_n.method.d_Ljava_la
ng_String__Ljava_lang_String_
          (void)

{
  boolean bVar1;
  undefined4 puVar2;
  int iVar3;
  undefined4 puVar4;
  undefined4[] ppuVar5;
  undefined4 unaff_v7;
  undefined4[][] pppuVar6;

                    /* cloudflare-dns.com */
  a.a(-0x38dcf826b942);
                    /* /dns-query?name=%s&type=A */
  a.a(-0x38eff826b942);
  puVar4 = new undefined4();
                    /* cloudflare-dns.com */
  puVar2 = a.a(-0x3909f826b942);
  puVar4.c(puVar2);
  puVar4.f(false);
                    /* /dns-query?name=%s&type=A */
  puVar2 = a.a(-0x391cf826b942);
  ppuVar5 = new undefined4[1];
  ppuVar5[0] = unaff_v7;
  puVar2 = String.format(puVar2,ppuVar5);
  puVar4.d(puVar2);
  puVar4.h(true);
  puVar4.e(0x1bb);
  pppuVar6 = new undefined4[1];
  ppuVar5 = new undefined4[2];
                    /* Accept */
  puVar2 = a.a(-0x3936f826b942);
  ppuVar5[0] = puVar2;
                    /* application/dns-json */
  puVar2 = a.a(-0x393df826b942);
  ppuVar5[1] = puVar2;
  pppuVar6[0] = ppuVar5;
  puVar4.b(pppuVar6);
  bVar1 = puVar4.i();
  if (bVar1 == false) {
    return null;
  }
  puVar2 = puVar4.a();
  puVar4 = new undefined4(puVar2);
                    /* Answer */
  puVar2 = a.a(-0x3952f826b942);
  puVar2 = puVar4.getJSONArray(puVar2);
```

FluBot zararlısının bir diğer özelliği cep telefonu numaralarında bulunan ülke bazlı kodları kullanarak o ülkeye ait spesifik saldırılar gerçekleştirmektir. Phishing saldırısı sırasında o ülkede bulunan kargo servisleri ve konuşulan dil saldırganlar tarafından dikkate alınmakta ve buna uygun bir ara yüz seçilmektedir.

```
aDropdownMenu:  .string "dropdown_menu",0 # String #13564 (0x34fc)
                .byte 0x18
aDsAsterisk20Tc:.string "ds-asterisk20.tcsbank.ru",0
                                        # DATA XREF: TelephonyWebSocketParserAvayaImpl_fetchWebSocketURL@LLL+12↓r
                                        # String #13565 (0x34fd)
                .byte 0x1D
aDsAsterisk20Tc_0:.string "ds-asterisk20.tcsbank.ru:8089",0
                                        # DATA XREF: TelephonyWebSocketParserAvayaImpl_fetchWebSocketURL@LLL+E↓r
                                        # String #13566 (0x34fe)
```

Decompile edilen FluBot görselinde görüldüğü gibi bu örnekte Rusya'da bulunan hedefleri seçmiştir.

```
v9, v8, _39K_A02
v0, aTxnamount # "txnAmount"
{v9, v0}, <ref JSONObject.optString(ref)
v11

v9, v8, _39K_A02
v0, aAppid # "appId"
{v9, v0}, <ref JSONObject.optString(ref)
v12

v9, v8, _39K_A02
v0, aDeviceid # "deviceId"
{v9, v0}, <ref JSONObject.optString(ref)
v13

v9, v8, _39K_A02
v0, aMobilenumber # "mobileNumber"
{v9, v0}, <ref JSONObject.optString(ref)
v14

v9, v8, _39K_A02
v0, aPayeraddr # "payerAddr"
{v9, v0}, <ref JSONObject.optString(ref)
v15

v9, v8, _39K_A02
v0, aPayeeaddr # "payeeAddr"
{v9, v0}, <ref JSONObject.optString(ref)
v16
```

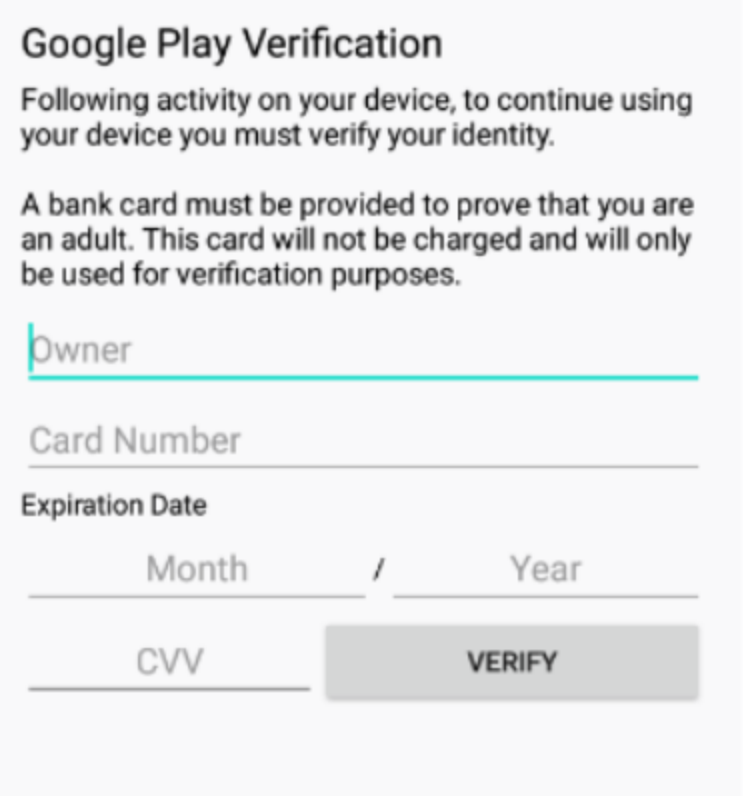
Hedef kullanıcıdan kredi kartı numarası, CVV, cihaz bilgisi gibi bilgileri çalmaktadır.

```
aEditcard:      .string "editCard",0    # DATA XREF: CardFragment_access$getEditCard$p@LL:loc_24E2AE↓r
                                        # CardFragment_showContentLoading@VZ+24↓r ...
                                        # String #13578 (0x350a)
                .byte  0xF
aEditcardNumber:.string "editCard.number",0
                                        # DATA XREF: CardFragment$e$a_invoke@L+2C↓r
                                        # String #13579 (0x350b)
                .byte    8
aEdittext:      .string "editText",0    # DATA XREF: SmartInputLayout_f@VLLZIL+26↓r
                                        # OtpInputEditText_getUnformattedText@L:loc_1EDD00↓r ...
                                        # String #13580 (0x350c)
                .byte  0xD
aEdittextText:  .string "editText.text",0
                                        # DATA XREF: OtpInputEditText_getUnformattedText@L+18↓r
                                        # String #13581 (0x350d)
                .byte 0x12
aEdittextbackgr:.string "editTextBackground",0 # String #13582 (0x350e)
                .byte  0xD
aEdittextcolor: .string "editTextColor",0 # String #13583 (0x350f)
                .byte  0xD
aEdittextstyle: .string "editTextStyle",0 # String #13584 (0x3510)
                .byte  0xA
aEditQuery:     .string "edit_query",0  # String #13585 (0x3511)
                .byte    9
aEditText:      .string "edit_text",0   # DATA XREF: SmartInputLayout_getEditText@L+12↓r
                                        # String #13586 (0x3512)
```

Phishing yöntemi ile kandırılan hedef kullanıcı bu bilgileri FluBot zararlısı içinde bulunan form arayüzüne girdikten sonra “GetCredential_A05” fonksiyonu ile String veriler saldırganlara iletilmektedir.

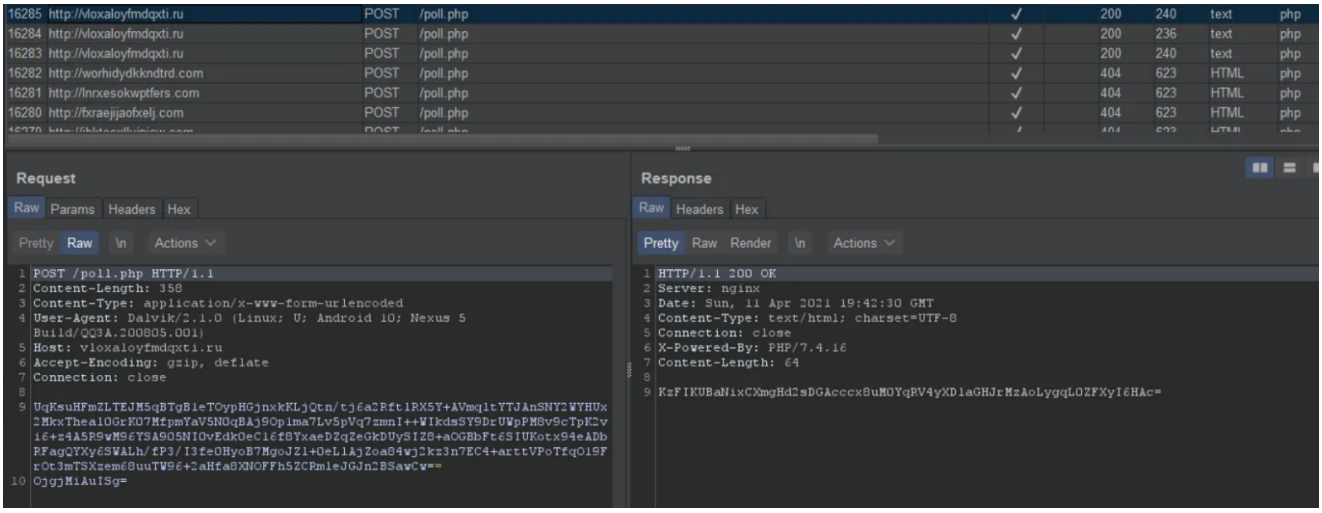
```
v8, v1, <t: String[]>
v0, aAtmpin # "ATMPIN"
v0, v8, v4
v0, aSmsEmailHotpTo # "SMS|EMAIL|HOTP|TOTP"
v0, v8, v2
v0, aMpin # "MPIN"
v0, v8, v5
v7, v1, <t: String[]>

v0, v3, GetCredential_A05
v0, loc_11ADFC
```

FluBot zararlısı tarafından hedef kullanıcıdan istenilen verilere ilişkin form (Phishing formu) aşağıdaki görselde yer almaktadır.



FluBot 3.7 Versiyonuna Ait HTTP Trafik Analizi

HTTP bağlantısını Burp Suite Proxy ile yakalamak için Frida kullanılarak zararlı yazılıma JavaScript kodu enjekte edilir bu sayede bağlantı yakalanabilmekte ve Android SSL Pinning bypass edilmektedir. Bağlantı incelendiği zaman poll.php üzerinden base64 ile encode edilmiş String veriler ile hedef cihazdan bağlantı isteklerinin gönderildiği göze çarpmaktadır. POST ve GET istekleri ile saldırganlar anlık olarak kurban cihaz ile haberleşmektedir.



4- MITRE ATT&CK Teknik ve Taktikleri (Android Cihaz İçin)

Tactic	Technique ID	Technique Name

Defense Evasion	T1418 T1406	1. Application Discovery 2. Obfuscated Files or Information
Credential access	T1409	1.Access Stored Application Data
Discovery	T1421 T1422 T1430 T1418 T1426	1.System Network Connections Discovery 2. System Network Configuration Discovery 3. Location Tracking 4. Application Discovery 5. System Information Discovery
Collection	T1432 T1430 T1507 T1409	1. Access Contact List 2. Location Tracking 3. Network Information Discovery 4. Access Stored Application Data
Command and Control	T1573 T1071 T1571 T1219	1. Encrypted Channel 2. Application Layer Protocol 3. Non-standard Port 4. Remote Access Software
Impact	T1447 T1448	1. Delete Device Data 2. Carrier Billing Fraud

5 – IOC Verisi

FluBot v3.7

Phishing Correos Hash Verileri
446833e3f8b04d4c3c2d2288e456328266524e396adbfeba3769d00727481e80
bb85cd885fad625bcd2899577582bad17e0d1f010f687fc09cdeb8fe9cc6d3e1
8c14d5bc5175c42c8dd65601b4964953f8179cfe5e627e5c952b6afd5ce7d39d
Phishing Fedex Hash Verileri

a601164199bbf14c5adf4d6a6d6c6de20f2ab35ec7301588bceb4ee7bb7d1fdc
f0fa95c3b022fb4fee1c2328ffbc2a9567269e5826b221d813349ebf980b34da
07ba6893c4ffc95638d4d1152f7c5b03aca4970474a95bf50942c619aa4382ae
ca5ba6098a2a5b49c82b7351920966009a99444da4d6f6e5a6649e5e2aeb3ff8
8be8576c742f31d690d449ab317b8fb562d03bc7c9dc33fa5abf09099b32d7a0
Phishing DHL Hash Verileri
54ecabbff30b05a6a97531f7dec837891ce49ae89878eaf38714c1874f5f1d15
c3838f9544e613917068f1b2e22ab647fd5a60701e1045b713767a92cf79f983
ab29813b1da1da48b4452c849eedc35b6c52044946d39392530573c540916f74

FluBot v4.0

Phishing DHL Hash Verileri
3a4bdcb1071e8c29c62778101b7ae8746f3ee57cb1588e84d7ee1991964703e6
22025590bbb4d3a30658fea45a936b6a346479c83d1c35f85521a1ac564342a0
774acbfbedd2a37e636f6251af84a7abb2e64c2db9d6de5ce0fec4121064ea49
3bf82acb8d511bfef3e083b73136824aab3612b516f150d916fe351b7e5bc9d3
9b9b67a2b9ec5a15044430a9f5d9ce6a7f524e1feed186a96309256df686cfdd
8bb8b1a1dc1487db610700f6b59ea4ab44ddc2f52e0eca06f8d1da663b312b58