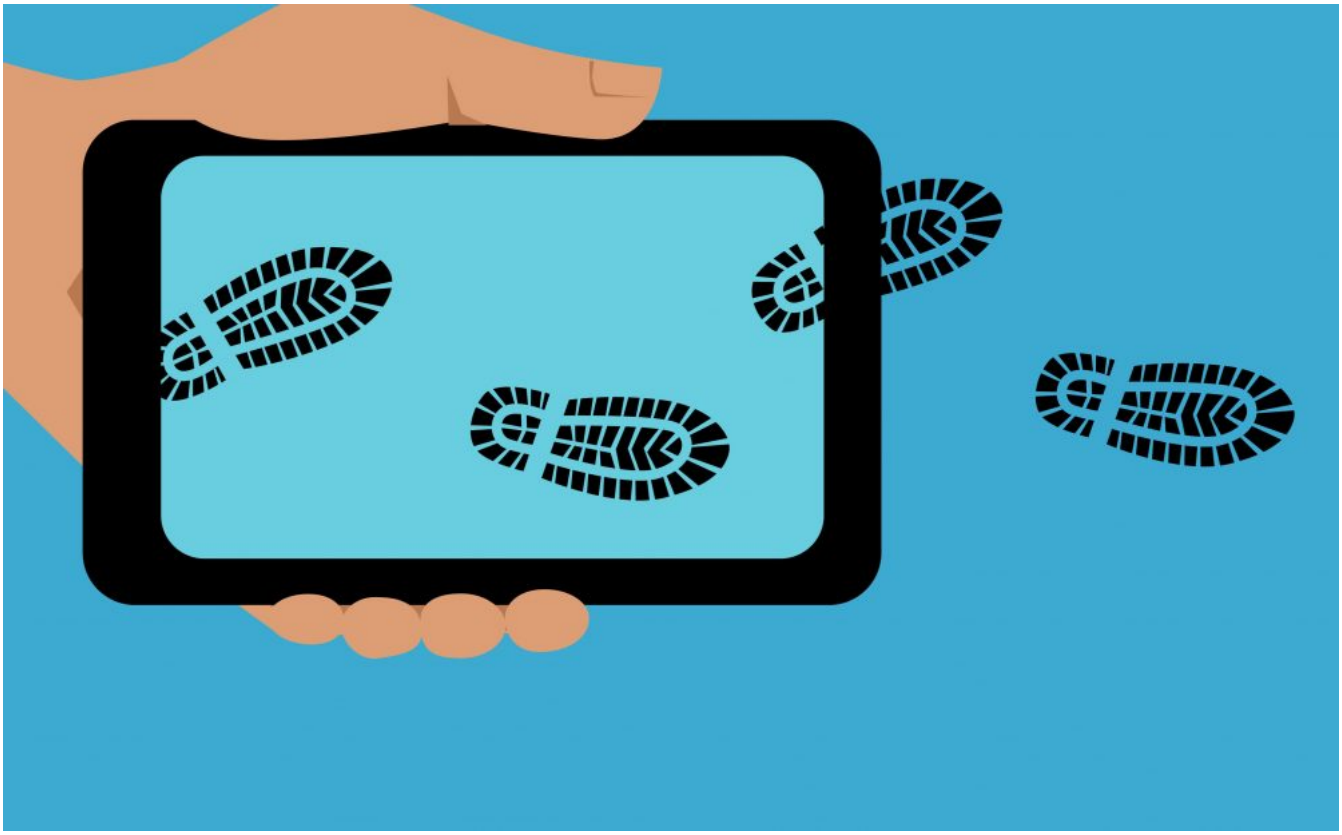
Tracking down the developer of Android adware affecting millions of users

welivesecurity.com/2019/10/24/tracking-down-developer-android-adware/

October 24, 2019



ESET researchers discovered a year-long adware campaign on Google Play and tracked down its operator. The apps involved, installed eight million times, use several tricks for stealth and persistence.

Lukas Stefanko
24 Oct 2019 - 11:30AM

ESET researchers discovered a year-long adware campaign on Google Play and tracked down its operator. The apps involved, installed eight million times, use several tricks for stealth and persistence.

We detected a large adware campaign running for about a year, with the involved apps installed eight million times from Google Play alone.

We identified 42 apps on Google Play as belonging to the campaign, which had been running since July 2018. Of those, 21 were still available at the time of discovery. We reported the apps to the Google security team and they were swiftly removed. However, the apps are still available in third-party app stores. ESET detects this adware, collectively, as Android/AdDisplay.Ashas.

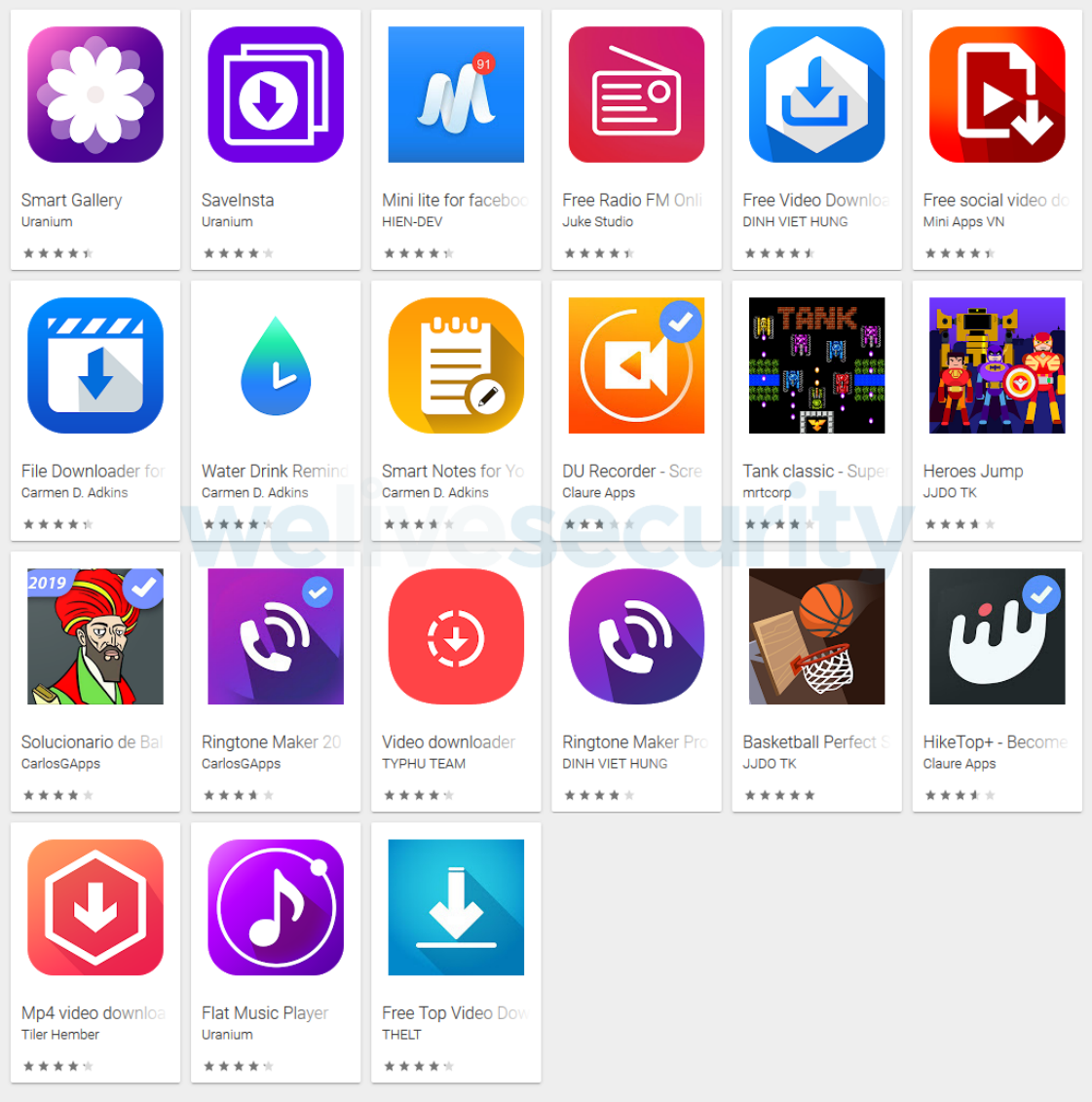


Figure 1. Apps of the Android/AdDisplay.Ashas family reported to Google by ESET

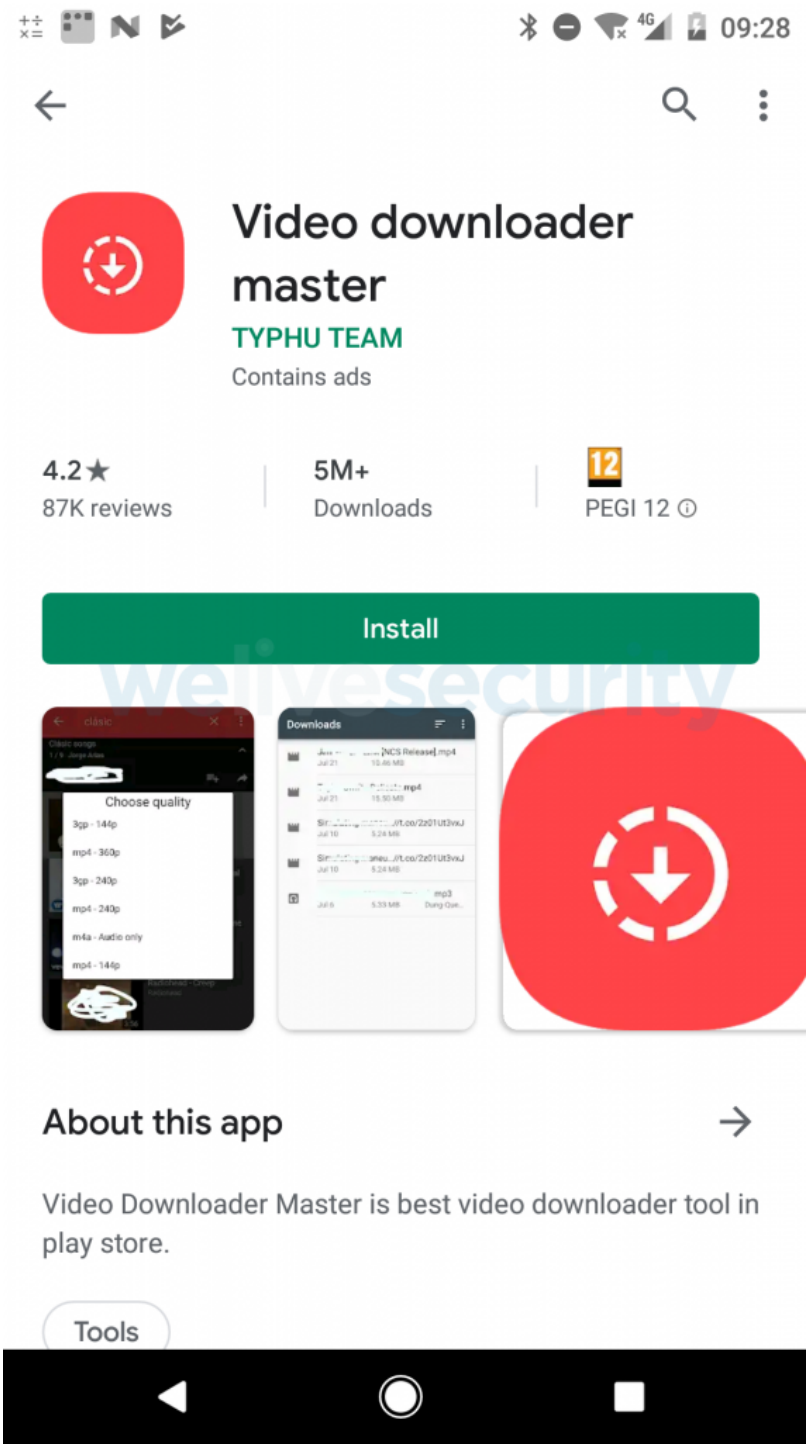


Figure 2. The most popular member of the Android/AdDisplay.Ashas family on Google Play was "Video downloader master" with over five million downloads

Ashas functionality

All the apps provide the functionality they promise, besides working as adware. The adware functionality is the same in all the apps we analyzed. [Note: The analysis of the functionality below describes a single app, but applies to all apps of the Android/AdDisplay.Ashas family.]

Once launched, the app starts to communicate with its C&C server (whose IP address is base64-encoded in the app). It sends "home" key data about the affected device: device type, OS version, language, number of installed apps, free storage space, battery status, whether the device is rooted and *Developer mode* enabled, and whether Facebook and FB Messenger are installed.

Figure 3. Sending information about the affected device

The app receives configuration data from the C&C server, needed for displaying ads, and for stealth and resilience.

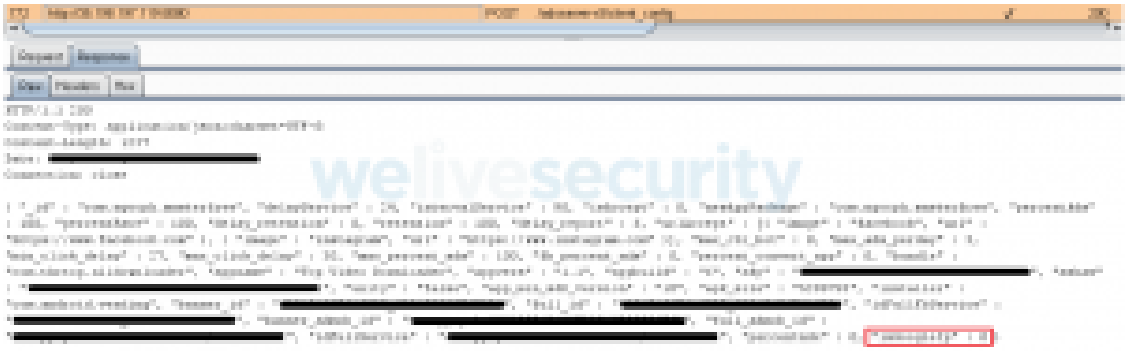


Figure 4. Configuration file received from the C&C server

As for stealth and resilience, the attacker uses a number of tricks.

First, the malicious app tries to determine whether it is being tested by the Google Play security mechanism. For this purpose, the app receives from the C&C server the *isGoogleIp* flag, which indicates whether the IP address of the affected device falls within the range of known IP addresses for Google servers. If the server returns this flag as positive, the app will not trigger the adware payload.

Second, the app can set a custom delay between displaying ads. The samples we have seen had their configuration set to delay displaying the first ad by 24 minutes after the device unlocks. This delay means that a typical testing procedure, which takes less than 10 minutes, will not detect any unwanted behavior. Also, the longer the delay, the lower the risk of the user associating the unwanted ads with a particular app.

Third, based on the server response, the app can also hide its icon and create a shortcut instead. If a typical user tries to get rid of the malicious app, chances are that only the shortcut ends up getting removed. The app then continues to run in the background without the user's knowledge. This stealth technique has been gaining popularity among adware-related threats distributed via Google Play.

Figure 5. Time delay to postpone displaying ads implemented by the adware

Once the malicious app receives its configuration data, the affected device is ready to display ads as per the attacker's choice; each ad is displayed as a full screen activity. If the user wants to check which app is responsible for the ad being displayed, by hitting the "Recent apps" button, another trick is used: the app displays a Facebook or Google icon, as seen in Figure 6. The adware mimics these two apps to look legitimate and avoid suspicion – and thus stay on the affected device for as long as possible.

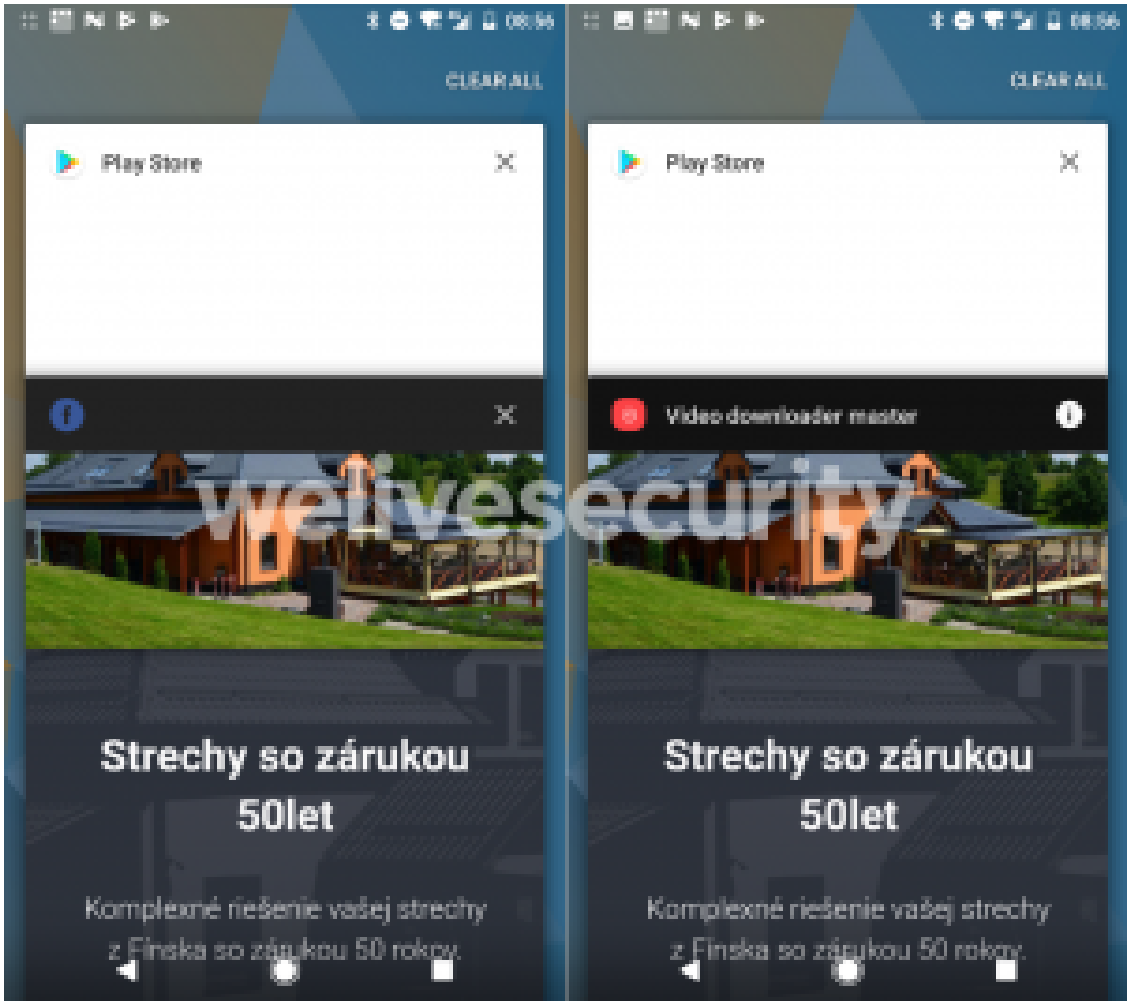


Figure 6. The adware activity impersonates Facebook (left). If the user long-presses the icon, the name of the app responsible for the activity is revealed (right).

Finally, the Ashas adware family has its code hidden under the *com.google.xxx* package name. This trick – posing as a part of a legitimate Google service – may help avoid scrutiny. Some detection mechanisms and sandboxes may whitelist such package names, in an effort to prevent wasting resources.

Figure 7. Malicious code hidden in a package named "com.google"

Hunting down the developer

Using open-source information, we tracked down the developer of the adware, who we also identified as the campaign's operator and owner of the C&C server. In the following paragraphs, we outline our efforts to discover other applications from the same developer and protect our users from it.

First, based on information that is associated with the registered C&C domain, we identified the name of the registrant, along with further data like country and email address, as seen in Figure 8.

[redacted]@gmail.com is associated to this person

Name	[redacted]
Address	[redacted] map
City	Ha Noi
State	Ha Noi
Country	Vietnam
Phone	+84.94[redacted]
Fax	+1.661[redacted]
Private	no

List of domain names registred by [redacted]@gmail.com

Domain Name	Creation Date	Registrar
minigameshouse.us	2018-07-26	namecheap.com

Figure 8. Information about the C&C domain used by the Ashas adware

Knowing that the information provided to a domain registrar might be fake, we continued our search. The email address and country information drove us to a list of students attending a class at a Vietnamese university – corroborating the existence of the person under whose name the domain was registered.

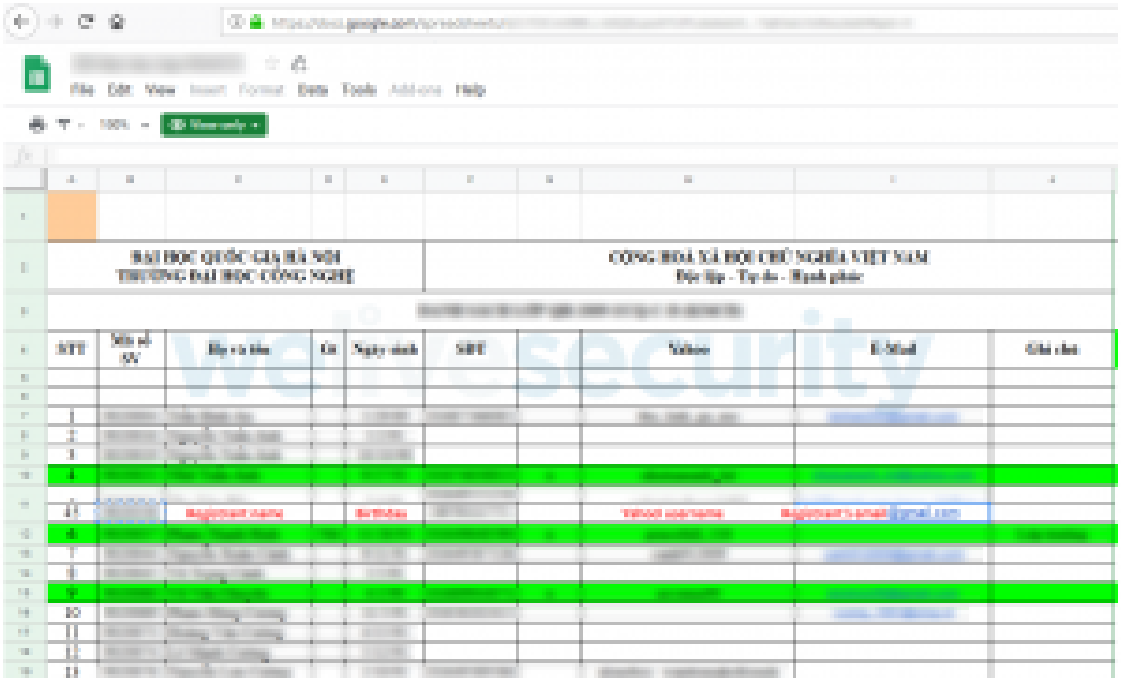


Figure 9. A university class student list including the C&C domain registrant

Due to poor privacy practices on the part of our culprit's university, we now know his date of birth (probably: he seemingly used his birth year as part of his Gmail address, as further partial confirmation), we know that he was a student and what university he attended. We were also able to confirm that the phone number he provided to the domain registrar was genuine. Moreover, we retrieved his University ID; a quick googling showed some of his exam grades. However, his study results are out of the scope of our research.

Based on our culprit's email address, we were able to find his GitHub repository. His repository proves that he is indeed an Android developer, but it contained no publicly available code of the Ashas adware at the time of writing of this blogpost.

However, a simple Google search for the adware package name returned a "TestDelete" project that had been available in his repository at some point

The malicious developer also has apps in Apple's App Store. Some of them are iOS versions of the ones removed from Google Play, but none contain adware functionality.

Figure 10. The malicious developer's apps published on the App Store which don't contain the Ashas adware

Searching further for the malicious developer's activities, we also discovered his Youtube channel propagating the Ashas adware and his other projects. As for the Ashas family, one of the associated promotional videos, "Head Soccer World Champion 2018 – Android, ios" was viewed almost three million times and two others reached hundreds of thousands of views, as seen in Figure 11.

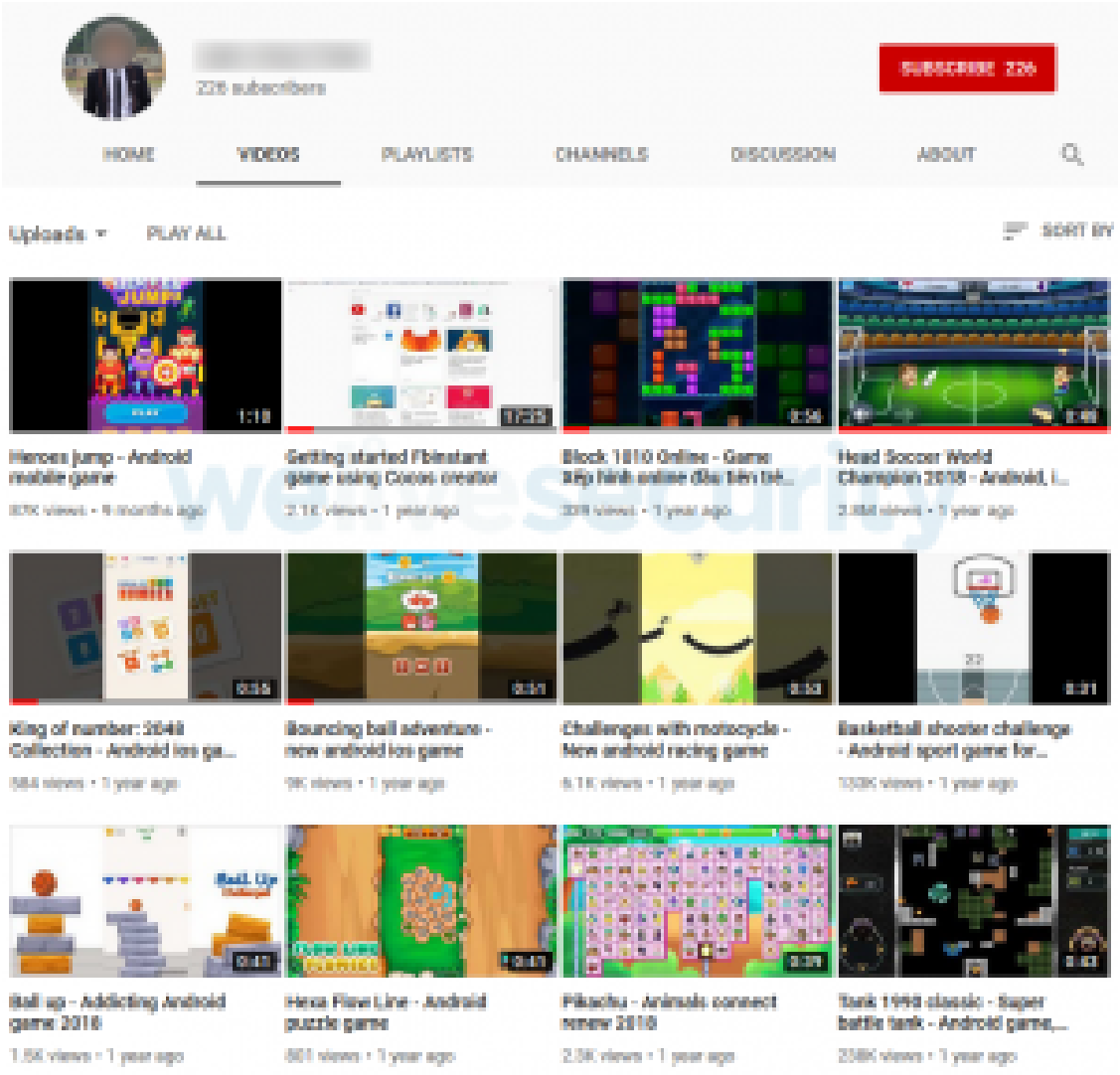


Figure 11. YouTube channel of the malicious developer

His YouTube channel provided us with another valuable piece of information: he himself features in a video tutorial for one of his other projects. Thanks to that project, we were able to extract his Facebook profile – which lists his studies at the aforementioned university.

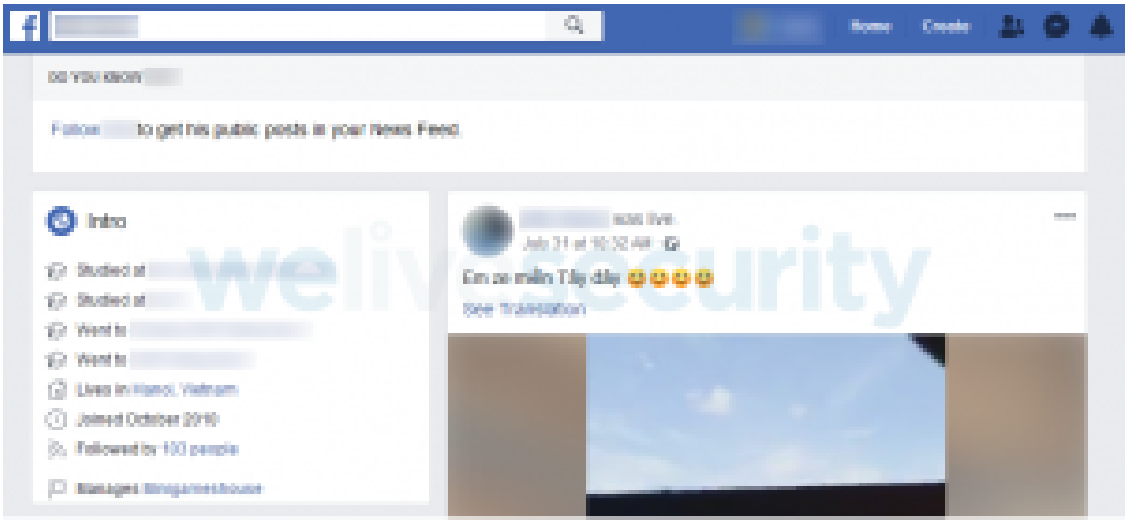


Figure 12. Facebook profile of the C&C domain registrar (cover picture and profile picture edited out)

Linked on the malicious developer's Facebook profile, we discovered a Facebook page, *Minigameshouse*, and an associated domain, minigameshouse[.]net. This domain is similar to the one the malware author used for his adware C&C communication, minigameshouse[.]us.

Checking this *Minigameshouse* page further indicates that this person is indeed the owner of the minigameshouse[.]us domain: the phone number registered with this domain is the same as the phone number appearing on the Facebook page.

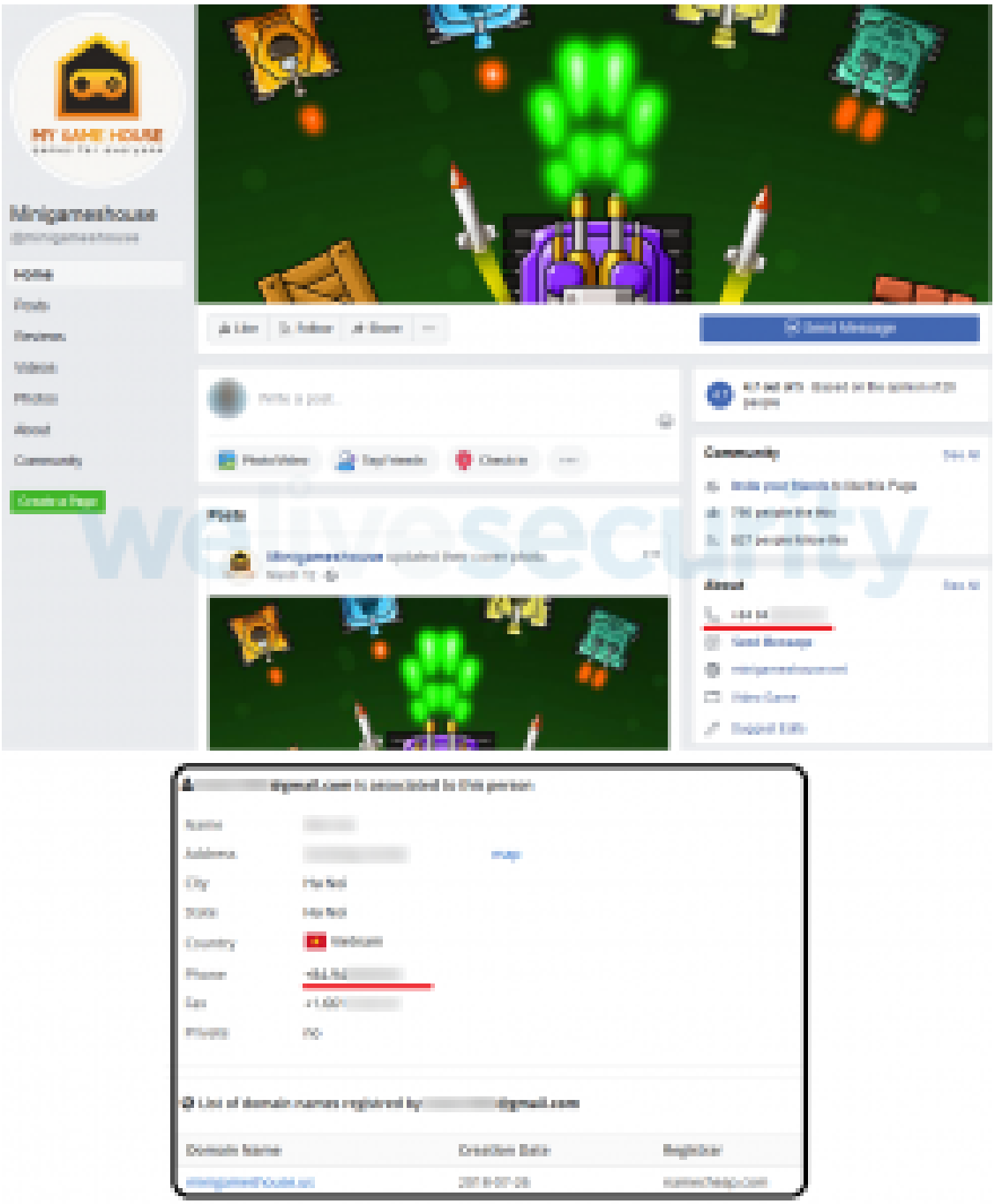


Figure 13. Facebook page managed by the C&C domain registrant uses the same base domain name (minigameshouse) and phone number as the registered malicious C&C used by the Ashas adware

Of interest is that on the *Minigameshouse* Facebook page, the malicious developer promotes a slew of games beyond the Ashas family for download on both Google Play and the App Store. However, all of those have been removed from Google Play – despite the fact that some of them didn't contain any adware functionality.

On top of all this, one of the malicious developer's YouTube videos – a tutorial on developing an "Instant Game" for Facebook – serves as an example of operational security completely ignored. We were able to see that his recently visited web sites were Google Play pages belonging to apps containing the Ashas adware. He also used his email account to log into various services in the video, which identifies him as the adware domain owner, beyond any doubt.

Thanks to the video, we were even able to identify three further apps that contained adware functionality and were available on Google Play.

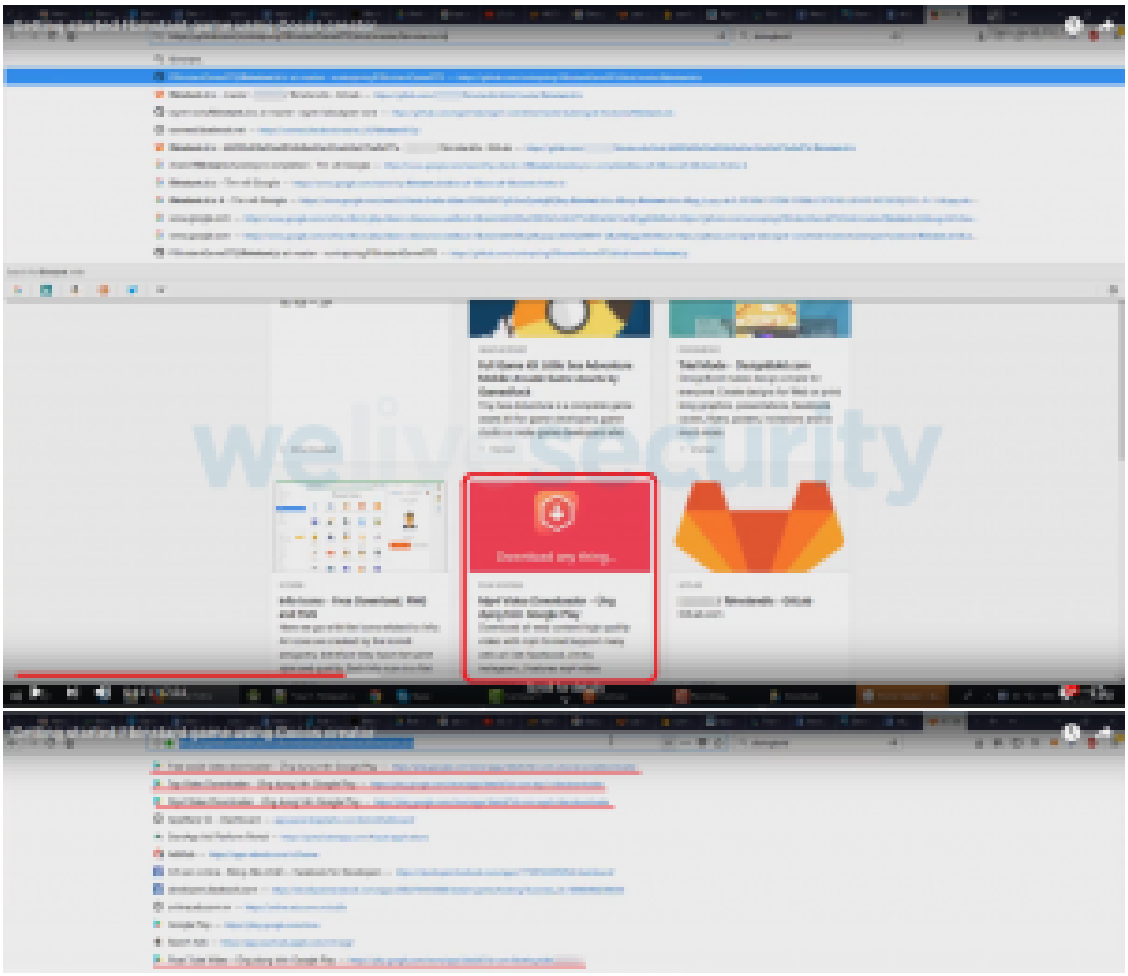


Figure 14. Screenshots from this developer's YouTube video shows history of checking Ashas adware on Google Play

ESET telemetry

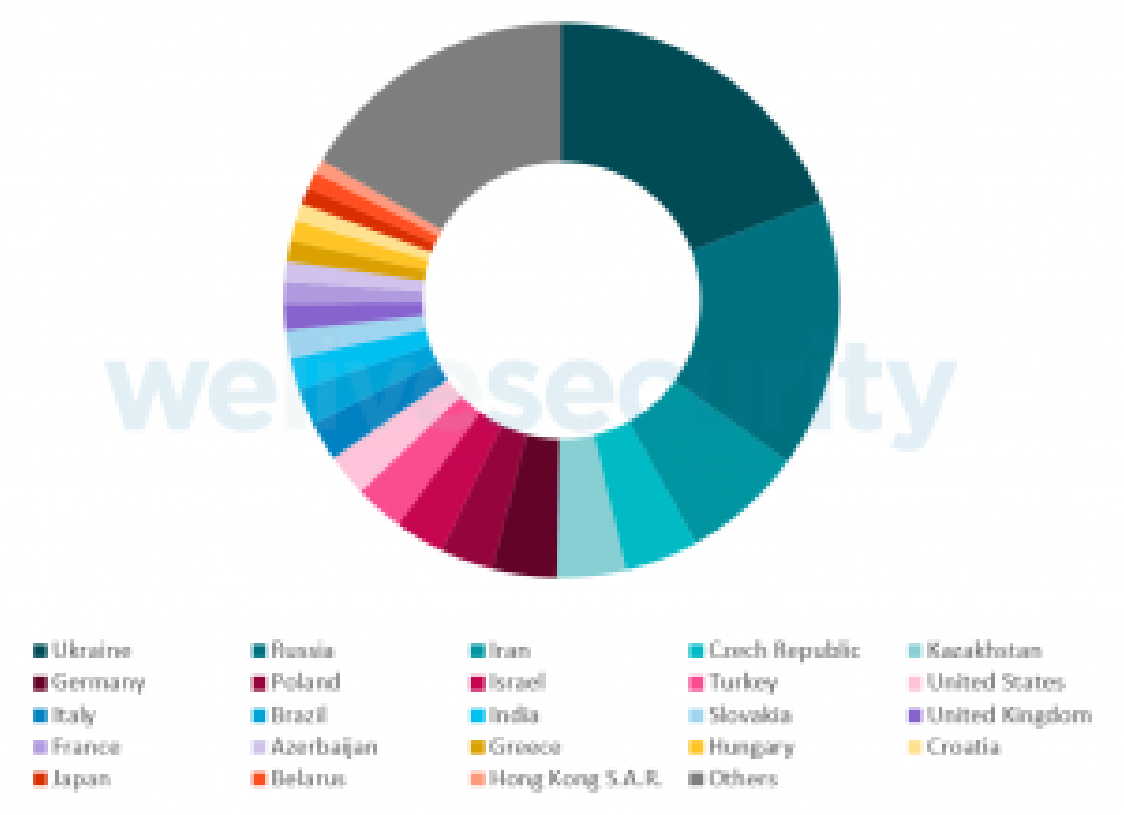


Figure 15. ESET detections of Android/AdDisplay.Ashas on Android devices by country

Is adware harmful?

Because the real nature of apps containing adware is usually hidden to the user, these apps and their developers should be considered untrustworthy. When installed on a device, apps containing adware may, among other things:

- Annoy users with intrusive advertisements, including scam ads
- Waste the device's battery resources
- Generate increased network traffic
- Gather users' personal information
- Hide their presence on the affected device to achieve persistence
- Generate revenue for their operator without any user interaction

Conclusion

Based solely on open source intelligence, we were able to trace the developer of the Ashas adware and establish his identity and discover additional related adware-infected apps. Seeing that the developer did not take any measures to protect his identity, it seems likely that his intentions weren't dishonest at first – and this is also supported by the fact that not all his published apps contained unwanted ads.

At some point in his Google Play "career", he apparently decided to increase his ad revenue by implementing adware functionality in his apps' code. The various stealth and resilience techniques implemented in the adware show us that the culprit was aware of the malicious nature of the added functionality and attempted to keep it hidden.

Sneaking unwanted or harmful functionality into popular, benign apps is a common practice among "bad" developers, and we are committed to tracking down such apps. We report them to Google and take other steps to disrupt malicious campaigns we discover. Last but not least, we publish our findings to help Android users protect themselves.

Indicators of Compromise (IoCs)

Package name	Hash	Installs
com.ngocph.masterfree	c1c958afa12a4fceb595539c6d208e6b103415d7	5,000,000+
com.mghstudio.ringtonemaker	7a8640d4a766c3e4c4707f038c12f30ad7e21876	500,000+
com.hunghh.instadownloader	8421f9f25dd30766f864490c26766d381b89dbee	500,000+
com.chungit.tank1990	237f9bfe204e857abb51db15d6092d350ad3eb01	500,000+
com.video.downloadmasterfree	43fea80444befe79b55e1f05d980261318472dff	100,000+
com.massapp.instadownloader	1382c2990bdce7d0aa081336214b78a06fceef62	100,000+
com.chungit.tankbattle	1630b926c1732ca0bb2f1150ad491e19030bcbf2	100,000+
com.chungit.basketball	188ca2d47e1fe777c6e9223e6f0f487cb5e98f2d	100,000+
com.applecat.worldchampion2018	502a1d6ab73d0aaa4d7821d6568833028b6595ec	100,000+
org.minigamehouse.photoalbum	a8e02fbd37d0787ee28d444272d72b894041003a	100,000+
com.mngh.tuanvn.fbvideodownloader	035624f9ac5f76cc38707f796457a34ec2a97946	100,000+
com.v2social.socialdownloader	2b84fb67519487d676844e5744d8d3d1c935c4b7	100,000+
com.hikeforig.hashtag	8ed42a6bcb14396563bb2475528d708c368da316	100,000+
com.chungit.heroesjump	c72e92e675afceca23bbe77008d921195114700c	100,000+
com.mp4.video.downloader	61E2C86199B2D94ABF2F7508300E3DB44AE1C6F1	100,000+
com.videotomp4.downloader	1f54e35729a5409628511b9bf6503863e9353ec9	50,000+
boxs.puzzles.Puzzlebox	b084a07fdfd1db25354ad3afea6fa7af497fb7dc	50,000+
com.intatwitfb.download.videodownloader	8d5ef663c32c1dbcdd5cd7af14674a02fed30467	50,000+
com.doscreenrecorder.screenrecorder	e7da1b95e5ddfd2ac71587ad3f95b2bb5c0f365d	50,000+
com.toptools.allvideodownloader	32E476EA431C6F0995C75ACC5980BDBEF07C8F7F	50,000+
com.top1.videodownloader	a24529933f57aa46ee5a9fd3c3f7234a1642fe17	10,000+
com.santastudio.headsoccer2	86d48c25d24842bac634c2bd75dbf721bcf4e2ea	10,000+
com.ringtonemakerpro.ringtonemakerapp2019	5ce9f25dc32ac8b00b9abc3754202e96ef7d66d9	10,000+
com.hugofq.solucionariodebaldor	3bb546880d93e9743ac99ad4295ccaf982920260	10,000+
com.anit.bouncingball	6e93a24fb64d2f6db2095bb17afa12c34b2c8452	10,000+
com.dktools.liteforfb	7bc079b1d01686d974888aa5398d6de54fd9d116	10,000+
net.radiogroup.tvnradio	ba29f0b4ad14b3d77956ae70d812eae6ac761bee	10,000+
com.anit.bouncingball	6E93A24FB64D2F6DB2095BB17AFA12C34B2C8452	10,000+
com.floating.tube.bymuicv	6A57D380CDDCD4726ED2CF0E98156BA404112A53	10,000+
org.cocos2dx.SpiderSolitaireGames	adbb603195c1cc33f8317ba9f05ae9b74759e75b	5,000+
games.puzzle.crosssum	31088dc35a864158205e89403e1fb46ef6c2c3cd	5,000+

Package name	Hash	Installs
dots.yellow.craft	413ce03236d3604c6c15fc8d1ec3c9887633396c	5,000+
com.tvngroup.ankina.reminderWater	5205a5d78b58a178c389cd1a7b6651fe5eb7eb09	5,000+
com.hdevs.ringtonemaker2019	ba5a4220d30579195a83ddc4c0897eec9df59cb7	5,000+
com.carlosapps.solucionariodebaldor	741a95c34d3ad817582d27783551b5c85c4c605b	5,000+
com.mngh1.flatmusic	32353fae3082eaeedd6c56bb90836c89893dc42c	5,000+
com.tvn.app.smartnote	ddf1f864325b76bc7c0a7cfa452562fe0fd41351	1,000+
com.thrtop.alldownloader	f46ef932a5f8e946a274961d5bdd789194bd2a7d	1,000+
com.anthu91.soccercard	0913a34436d1a7fcd9b6599fba64102352ef2a4a	1,000+
com.hugofq.wismichudosmildiecisiete	4715bd777d0e76ca954685eb32dc4d16e609824f	1,000+
com.gamebasketball.basketballperfectshot	e97133aaf7d4bf90f93fefb405cb71a287790839	1,000+
com.nteam.solitairefree	3095f0f99300c04f5ba877f87ab86636129769b1	100+
com.instafollowers.hiketop	3a14407c3a8ef54f9cba8f61a271ab94013340f8	1+

C&C server

http://35.198.197[.]119:8080

MITRE ATT&CK techniques

Tactic	ID	Name	Description
Initial Access	T1475	Deliver Malicious App via Authorized App Store	The malware impersonates legitimate services on Google Play
Persistence	T1402	App Auto-Start at Device Boot	An Android application can listen for the BOOT_COMPLETED broadcast, ensuring that the app's functionality will be activated every time the device starts
Impact	T1472	Generate Fraudulent Advertising Revenue	Generates revenue by automatically displaying ads

Kudos to @jaymin9687 for bringing the problem of unwanted ads in the “Video downloader master” app to our attention.

24 Oct 2019 - 11:30AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion