Practical FOFA Asset Expansion: APT-C-23 Android Malware

medium.com/@fofabot/practical-fofa-asset-expansion-apt-c-23-android-malware-7964b6625c6d

Fofabot February 4, 2024

Fofabot

--

Overview

This content focuses on a deep analysis of the malicious activities of APT-C-23 on the Android platform.

APT-C-23, also known as Arid Viper, Frozen Cell, Desert Falcon, mainly targets educational institutions, military institutions, and other important areas related to Middle Eastern countries. The cyber-attack activities are mainly aimed at stealing sensitive information and have the ability to attack multiple platforms such as Windows, Android, and iOS. Attackers usually use custom mobile malware to collect sensitive information from the target and deploy other malware on infected devices.

Through the analysis of three publicly disclosed IOCs, this study uses FOFA for asset extension. **Since the 7 obtained results were not covered by threat intelligence platforms, reverse analysis was carried out on the malicious APP obtained from the extension to confirm the authenticity of the extension results.**

In addition, through research and analysis, it has been found that the team mainly uses dating software for espionage. The malicious code of its application software is more hidden than the IOC source. The attacker makes it more difficult for users to discover this malicious behavior by continuously optimizing the Android code.

APT-C-23 Android IOC

The IOC comes from the articles “APT-C-23（双尾蝎）组织最新攻击活动分析” and “针对巴以地区围绕卡塔尔世界杯的攻击活动” from the 360 Threat Intelligence Center’s Fenhuo Lab.

https://blaxaplayer.com/
https://www.bbalignit.com/
https://kora442.com/

Extraction of FOFA Rules

According to the articles where the IOC was obtained, it can be clearly known that the method used by the APT-C-23 team is to modify some well-known APP applications and create corresponding phishing websites for payload delivery.

We first search for information related to the three phishing websites we obtained in FOFA.

According to the characteristics on FOFA, we can see that Blaxaplayer.com and bbalignit.com use the same certificate, but the certificate JARM fingerprint is not the same as kora442.com, so it cannot be used as a query rule.

Looking at other features, the two websites both use the LiteSpeed service, but no related content was found on kora442.com.

Therefore, we will focus on their website text. By viewing the website text and comparing the three phishing websites, we find that the beginning of the webpage contains the same features of keywords, description, and canonical.

These features are common, although they can be marked, but the results must be very large, so we need to continue to try to get other similar features from the original text of the website.
Check out the relevant parts of these three IOCs from their original text and find two features. One is getAppVersionOne(), and the other is getApp().

This is the prominent feature we found so far. We combine all the features to generate the FOFA query syntax. Please note here that special characters need to add escape characters.

status_code="200" && body=”name=\”keywords\”” && body=”name=\”description\”” && body=”rel=\”canonical\”” && (body=”onclick=\”getApp()\”” || body=”onclick=\”getAppVersionOne()\””)

You can see that 60 pieces of data and 15 independent IPs have been circled. However, when we verify one by one, we find that there is still redundant data, so we need to optimize this query statement again.
Now you can lock on to js. Js is a very useful feature when looking for similar feature websites. So we continue to filter on the basis of the above query statement, adding similar myScript.js, note that this is also an or relationship.

status_code=”200" && body=”name=\”keywords\”” && body=”name=\”description\”” && body=”rel=\”canonical\”” && (body=”onclick=\”getApp()\”” || body=”onclick=\”getAppVersionOne()\””) && (body=”src=\”js/myScript.js\”” || body=”src=\”assets/js/myScript.js\”” || body=”src=\”js/script.js\””)

In the end, 49 assets and 11 independent IPs were located.

After excluding the 3 phishing websites publicly available in the IOC and the phishing websites related to the World Cup, the remaining assets were deduplicated, and a total of 7 domain names were obtained, all of which were social application programs. However, in the process of further verifying the correctness of the results, we found a problem, so we need to verify the results of the extension one by one.

Result Verification

For the discovered unknown IOC, further verification is needed, but when comparing, it is found that the new IOC found is basically not covered on the threat intelligence platform, so we verify the obtained results one by one to confirm the authenticity of the IOC. See the appendix for the final verification results.

Analyzing the extension results one by one, all websites use exactly the same template to display their content, only the content, title, and pictures are slightly different, and the page features are extremely similar to our known phishing websites.

According to the analysis in the article we referred to, the phishing websites all have the myscript.js feature.

Thread Analysis 1

After analyzing the downloaded app, we found that the features of this app are not consistent with those in the source of IOC. There are no obvious code snippets like executecommands or WhatsApp information.

https://www.reblychat.com
https://clemochat.com
https://mail.wislisapp.com
https://mail.lapizachat.com

However, a connection may be gleaned from the report “Arid Viper disguising mobile spyware as updates for non-malicious Android applications” by the Cisco Threat Intelligence Research Team in October of the 23rd year.

The article says that some of the malware deployed by APT-C-23 uses Google’s Firebase platform as the C2 infrastructure for malicious applications.

Firebase platform mainly serves as the C2 channel to issue commands as well as download and upload files. The platform can also provide the malware with new C2 server addresses, so it can switch from the Firebase platform to another attacker-controlled C2 host.

One of the Firebase projects used by Arid Viper in this campaign can be traced back to 2021, and there are some non-malicious mobile APKs associated with it. This indicates that the operator has been trying to create, test, and promote other APK software for many years.

The team conducts espionage through a large number of dating software. The malicious code shown in the article was searched but no identical code snippets were found. It is suspected that the attacker has upgraded the code again to make the attack behavior more hidden.
Interestingly, among these apps, if one of the four apps is present, others cannot be installed. Therefore, these four apps can be judged to be the same set of apps in different skins.

We installed the applications on the emulator, and even with the Google framework, we were still prompted to update Google Play services.

And, these apps use the Firebase development platform, which is consistent with the description in the reference article.

In the code prompting Google Play to update, you can see the presence of multiple languages. From this, it can be judged that the target group is quite clear.

In addition, the getAntiSet method’s ANTI_SET contains a large number of Android device antivirus software package names, and combines them through splicing.

The checkValidation method in this class is used to determine whether to execute onchecked(true) by judging PackageManager.checkIfAppInstall.

Tracking PackageManager.checkIfAppInstall, you can see that this method is used to check whether a specific application is installed on the device. The value passed in is the antivirus software package name mentioned above. When these antivirus software are not in the app, it returns true.

Since our device does not have these antivirus software, the program executed onchecked(true) and finally returned true. Continue tracking to confirm the function of the code. It is used to confirm whether to update Google Play. When there is antivirus software, no update prompt is given. When there is no antivirus software, an update prompt is given.

When we perform an update, the malicious update package updatte.apk is stored in the files folder of these apps. When the victim clicks update, it will automatically install the malicious program for the victim.

After successful installation, it will record contact information.

Then use the HttpManager.sendProcess method to transmit information.

The sent data packet is as follows, the above four domain names all exist in this interface apps/indx.php

Analyzing the update.apk malicious program, its code is obfuscated, and it will request all permissions during installation.

At the same time, it will judge whether there is antivirus software in the Android device again.

There are also some other character stitching behaviors.

Some information can be found by stitching some character content.

The OooO00o method is responsible for building HTTP POST requests, sending GZIP compressed JSON data, and handling responses.

o00Oo0.OooOo is responsible for getting device information and uploading data to the server.

Thread Analysis 2

Analyzing the remaining two apps, vovanil installation failed, and the js of the two app websites is consistent with the above suspicious js.

https://wobomov.com/
https://voevanil.com/

The same routine, the same prompt needs to be updated during installation.

The location of the prompt update code is found below.

Looking up its reference, the onResume method checks the camera permission and when the application named GConfig.PT_PACKAGE_NAME is not installed, it calls the above showCustomDialog2 method to display a custom dialog box prompting for version updates.

Jumping to the place where GConfig.PT_PACKAGE_NAME is declared, the PT_PACKAGE_NAME field gets the final package name through splicing. After splicing, it shows that the package name is com.video.graphics. Therefore, this application will check whether another app is installed. If not, it will prompt to update and download com.video.graphics and install it for the user. The behavior pattern is consistent, so no further analysis is needed.

Thread Analysis 3

In addition to the above software, there is another phishing website targeting the World Cup in APT-C-23 in the data.

wcup22qat.com

Viewing the original text of this website through FOFA, except for the description such as icon, title, etc., it is exactly the same as the features shown in IOC.

By analyzing the attack mode and code features of the above applications, they all conform to the characteristics of APT-C-23. Therefore, it can be judged that the above apps and World Cup related phishing websites are all APT-C-23 related assets.

Summary

This research started with the analysis of 3 publicly available IOCs. Using FOFA's cyberspace mapping technology, we extended these IOCs. Because the 7 results obtained were not covered by threat intelligence platforms. Therefore, we decided to reverse analyze the malicious APP obtained by extension to confirm the authenticity of the extension results.

Through the extension analysis of some IOCs, we found that the team conducts espionage through a large number of dating software. The attacker has adopted very clever means, such as prompting to update Google Play store or software updates, to further plant malicious applications. Compared with the source of IOC, these malicious APP codes are more hidden and difficult to detect.

Attackers make it difficult for users to detect malicious behavior during normal use by continuously optimizing Android code, leading to personal information leakage. There are cybersecurity risks everywhere, like this malicious program disguised as dating software, it is a heavy disaster area for espionage worldwide.

References

1. [Arid Viper disguising mobile spyware as updates for non-malicious Android applications](https://blog.talosintelligence.com/arid-viper-mobile-spyware)
2. [针对巴以地区围绕卡塔尔世界杯的攻击活动](https://mp.weixin.qq.com/s/48Atw1b6Oe7A-vlsKHYWwg)
3. [APT-C-23（双尾蝎）组织最新攻击活动分析](https://mp.weixin.qq.com/s/NomfjAjGYdsOpLBtiOSZpA)

Appendix

IOC:
blaxaplayer.com
bbalignit.com
kora442.com
wcup22qat.com
reblychat.com
wobomov.com
voevanil.com
clemochat.com
wislisapp.com
lapizachat.com