

Phishing Attacks from Earth Empusa Reveal ActionSpy

By Ecular Xu, Joseph C Chen (words)

Published: 2020-06-11 · Archived: 2026-04-05 21:22:21 UTC

While tracking Earth Empusa, also known as [POISON CAR](#)[Popen on a new tab](#)/[Evil Eye](#)[open on a new tab](#), we identified an undocumented Android spyware we have named ActionSpy (detected by Trend Micro as AndroidOS_ActionSpy.HRX). During the first quarter of 2020, we observed Earth Empusa's activity targeting users in Tibet and Turkey before they extended their scope to include Taiwan. The campaign is reportedly targeting victims related to Uyghurs by compromising their Android and iOS mobile devices. This group is known to use watering hole attacks, but we recently observed them using phishing attacks to deliver their malware.

The malware that infects the mobile devices is found to be associated with a sequence of iOS exploit chain attacks in the wild [since 2016](#)[open on a new tab](#). In April 2020, we noticed a phishing page disguised as a download page of an Android video application that is popular in Tibet. The phishing page, which appears to have been copied from a third-party web store, may have been created by Earth Empusa. This is based on the fact that one of the malicious scripts injected on the page was hosted on a domain belonging to the group. Upon checking the Android application downloaded from the page, we found ActionSpy.



Figure 1. The Earth Empusa attack chain

ActionSpy, which may have been around since 2017, is an Android spyware that allows the attacker to collect information from the compromised devices. It also has a module designed for spying on instant messages by abusing [Android Accessibility](#)[open on a new tab](#) and collecting chat logs from four different instant messaging applications.

Phishing attacks delivering ActionSpy

Earth Empusa's use of phishing pages is similar to our recent report on [Operation Poisoned News](#)[news article](#), which also used web news pages as a lure to exploit mobile devices. Earth Empusa also used social engineering lures to trick its targets into visiting the phishing pages. We found some news web pages, which appear to have been copied from Uyghur-related news sites, hosted on their server in March 2020. All pages were injected with a script to load the cross-site scripting framework [BeEF](#)[Fopen on a new tab](#). We suspect the attacker used the framework to deliver their malicious script when they found a targeted victim browsing the said sites. However, our investigation did not yield any script when we attempted to access said phishing pages. How these pages were distributed in the wild is also unclear.



Figure 2. A news page copied from the World Uyghur Congress website used for loading the BeEF framework

Upon continued investigation in late April 2020, we found another phishing page that appears to be copied from a third-party web store and injected with two scripts to load [ScanBox](#)[open on a new tab](#) and BeEF frameworks. This phishing page invites users to download a video app that is known to Tibetan Android users. We believe the page was created by Earth Empusa because the BeEF framework was running on a domain that reportedly belongs to the group.

The download link was modified to an archive file that contains an Android application. Analysis then revealed that the application is an undocumented Android spyware we named ActionSpy.



  Figures 3 and 4. Fake Android application download page (In original language and translated into English)

 Figure 5. The injection of ScanBox (above) and BeEF (below) on the phishing page shows overlap to Earth Empusa's domain

Breaking Down ActionSpy

This malware impersonates a legitimate Uyghur video app called Ekran. The malicious app has the same appearance and features as the original app. It is able to achieve this with [VirtualAppopen on a new tab](#). In addition, it's also protected by [Bangcleopen on a new tab](#) to evade static analysis and detection.



Figure 6. ActionSpy's icon (left) and appearance (right)



Figure 7. ActionSpy is protected by Bangcle

A legitimate Ekran APK file is embedded in the ActionSpy assets directory, and installed in virtual environment after VirtualApp is ready when ActionSpy is launched the first time.

Figure 8 and 9. Install real "Ekran" (above) and launch it (below)

ActionSpy's configuration, including its C&C server address, is encrypted by DES. The decryption key is generated in native code. This makes static analysis difficult for ActionSpy.

Every 30 seconds, ActionSpy will collect basic device information like IMEI, phone number, manufacturer, battery status, etc., which it sends to the C&C server as a heartbeat request. The server may return some commands that will be performed on the compromised device. All the communication traffic between C&C and ActionSpy is encrypted by RSA and transferred via HTTP.



Figure 10. Collected device information

ActionSpy supports the following modules:

| Module Name | Description |
|-------------|---|
| location | Get device location latitude and longitude |
| geo | Get geographic area like province, city, district, street address |

| | |
|-----------------|--|
| contacts | Get contacts info |
| calling | Get call logs |
| sms | Get SMS messages |
| nettrace | Get browser bookmarks |
| software | Get installed APP info |
| process | Get running processes info |
| wifi connect | Make device connect to a specific Wi-Fi hotspot |
| wifi disconnect | Make the device disconnect to Wi-Fi |
| wifi list | Get all available Wi-Fi hotspots info |
| dir | Collect specific types of file list on SDCard, like txt, jpg, mp4, doc, xls... |
| file | Upload files from device to C&C server |
| voice | Record the environment |
| camera | Take photos with camera |
| screen | Take screenshot |
| wechat | Get the structure of WeChat directory |
| wxfile | Get files that received or sent from WeChat |
| wxrecord | Get chat logs of WeChat, QQ, WhatsApp, and Viber |

Abuse of Accessibility

Normally, a third-party app can't access files belonging to others on Android. This makes it difficult for ActionSpy to steal chat log files from messaging apps like WeChat directly without root permission. ActionSpy, in turn, adopts an indirect approach: it prompts users to turn on its Accessibility service and claims that it is a memory garbage cleaning service.



Figure 11. Prompt to turn on Accessibility

Once the user enables the Accessibility service, ActionSpy will monitor Accessibility events on the device. This occurs when [something “notable” happens on a new tab](#) in the user interface (such as clicked buttons, entered text, or changed views). When an Accessibility Event is received, ActionSpy checks if the event type is [VIEW_SCROLLED](#) or [WINDOW_CONTENT_CHANGED](#) and then check if the events came from targeted apps like WeChat, QQ, WhatsApp, and Viber. If all the above conditions are met, ActionSpy parses the current activity contents and extracts information like nicknames, chat contents, and chat time.

All the chat information is formatted and stored into a local SQLite Database. Once a “wxrecord” command is pushed, ActionSpy will gather chat logs in the database and convert them into JSON format before sending it to its C&C server.

 *Figure 12. Code snippet of parsing chat information*

We believe ActionSpy has existed for at least three years, based on its certificate sign time (2017-07-10). We also sourced some old ActionSpy versions that were created in 2017.



Figure 13. Certificate info



Figure 14. The earlier version (created in 2017)

More on Earth Empusa: Watering hole attacks to compromise iOS systems

Earth Empusa also employs watering hole attacks to compromise iOS devices. The group injected their malicious scripts on websites that their targets could potentially visit and load the injected script from it. We found two kinds of attacks they injected into compromised websites:

- One injection we found is the ScanBox framework. The framework can collect information from a website’s visitors by using JavaScript to record keypresses and harvest the profiles of the OS, browser, and browser plugins from the client environment. The framework is usually used during the reconnaissance stage, allowing them to understand their targets and prepare for the next stage of the attack.
- Another injection is their exploit chain framework, which exploits the vulnerabilities on the iOS devices. When a victim accesses the framework, it checks the User-Agent header of the HTTP request to determine the iOS version on the victim’s device and reply with a corresponding exploit code. If the User-Agent doesn’t belong to any of the targeted iOS versions, the framework will not deliver any additional payload.

 *Figure 15. An example of iOS exploit chain traffic*

In the first quarter of 2020, the exploit chain framework was upgraded to include a newer iOS exploit that can compromise iOS versions 12.3, 12.3.1, and 12.3.2. Other researchers have also [published](#) details of this updated exploit.

 *Figure 16. The script for determining the iOS version and launching the exploit code*

We have observed these injections on multiple Uyghur-related sites since the start of 2020. In addition, we have also identified a news website and political party website in Turkey that have been compromised and injected with the same attack. In a more recent development, we found the same injection on a university website as well as a travel agency site based in Taiwan in March 2020. These developments have led us to believe that Earth Empusa is widening the scope of their targets.

Best practices and solutions

Earth Empusa is still very active in the wild. We are constantly tracking and monitoring the threat group as it continues to develop new ways to attack its targets.

iOS users are advised to keep their devices updated. Android users, on the other hand, are encouraged to install apps only from trusted places such as Google Play to avoid malicious apps.

Users can also install security solutions, such as the [Trend Micro™ Mobile Security products](#), that can block malicious apps. End users can also benefit from their multilayered security capabilities that secure the device owner’s data and privacy, and features that protect them from ransomware, fraudulent websites, and identity theft.

For organizations, the [Trend Micro™ Mobile Security for Enterprise products](#) suite provides device, compliance and application management, data protection, and configuration provisioning. The suite also protects devices from attacks that exploit vulnerabilities, prevents unauthorized access to apps and detects and blocks malware and fraudulent websites. [Trend Micro’s Mobile App Reputation Service \(MARS\)](#) covers Android and iOS threats using leading sandbox and [machine learning](#) technologies to protect users against malware, zero-day and known exploits, privacy leaks, and application vulnerability.

Indicators of Compromise

All of the malicious apps below are detected as AndroidOS_ActionSpy.HRX.

| SHA256 | Package Name | Label |
|--|----------------------|-------------------------|
| 56a2562426e504f42ad9aa2bd53445d8e299935c817805b0d9b9431521769271 | com.omn.vvi | Ekran |
| b6e2fdbf022cd009585f62a3de71464014edd58125eb7bc15c2c670d6d5d3590 | com.isyiv.klxblnwc.r | 系统优化 |
| de6065c63f05f8cddaec2f43a3789cca7d8e16221bd04bf3ce8092809b146ebe | com.isyiv.klxblnwc.r | 系统优化 |
| 2117e2252fe268136a2833202d746d67bf592de819cc1600ac8d9f2738d8d4d6 | com.isyiv.klxblnwc | Service Runtime Library |
| 588b62a2e0bffa8935cd08ae46255a972b0af4966483967a3046a5df59d38406 | com.isyiv.klxblnwc | Service Runtime Library |
| d6478b4b7f0ea38947d894b1a87baf4bed7a1ece934fff9dfc233610de232814 | com.isyiv.klxblnwc | Service Runtime Library |
| 8d0a123e0fe91637fb41d9d9650a4b9c75b6ce77a2b51ac36f05a337da7afd80 | com.ecs.esap | Service Runtime Library |
| 9bc16f635fde4ff0b6b02b445a706d885779611b7813c5607ab88fdff43fcc2f | com.cd.weixin | VWechat |
| 334dbd15289aaef3763f1702003de52ff709515246902f51ee87a41467a8e55 | com.android.dmp.rec | Recording |

| | | |
|--|---------------------|-----------|
| 50c10ab93910a6e617c85a03f8c38a10a7c363e2d37b745964e696da8f98a93d | com.android.dmp.rec | Recording |
| 6575eeda2a8f76170fb6034944eeda5c88dac8009edccc880124fa729dd3c1fd | com.android.dmp.l | Location |
| eff30f6cc2d5d04ce4aef0c50f1fb375fb817a803bf3e8e08c847f04658185ba | com.android.dmp.l | Location |
| a0a48d7e0762ab24b2ec3ec488b011db866992db5392926fe43dd3d1c398e30d | com.android.dmp.cm | Camera |
| 088769a80b39d0da26c676a5a52eacbdb805dc67c8a85e562785c375c642b501 | com.android.dmp.c | Core |
| 87306b59aaba0ea92ea6a05feb9366eeb625e8da08ed3ef6c86a5cf394fada5 | com.android.dmp.c | Core |

| Indicator | Type |
|-----------------------------------|-----------------------------|
| gotossl.ml | Domain used by Earth Empusa |
| goforssl.top | Domain used by Earth Empusa |
| geo2ipapi.org | Domain used by Earth Empusa |
| appbuliki.com | Domain used by Earth Empusa |
| umutyole.com | Domain used by Earth Empusa |
| t.freenuun.com | Domain used by Earth Empusa |
| start.apiforssl.com | Domain used by Earth Empusa |
| bloomberg.com.cm | Domain used by Earth Empusa |
| static.apiforssl.com | Domain used by Earth Empusa |
| cdn.doublesclick.me | Domain used by Earth Empusa |
| static.doublesclick.info | Domain used by Earth Empusa |
| status.search-sslkey-flush.com | Domain used by Earth Empusa |
| http://114.215.41.93/ | ActionSpy C&C URL |
| http://static.doubles.click:8082/ | ActionSpy C&C URL |

MITRE ATT&CK Techniques



Source: <https://blog.trendmicro.com/trendlabs-security-intelligence/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa/>