BladeHawk group: Android espionage against Kurdish ethnic group

welivesecurity.com/2021/09/07/bladehawk-android-espionage-kurdish/

September 7, 2021

ESET researchers have investigated a mobile espionage campaign that targets the Kurdish ethnic group and has been active since at least March 2020

Lukas Stefanko
7 Sep 2021 - 02:30PM

ESET researchers have investigated a mobile espionage campaign that targets the Kurdish ethnic group and has been active since at least March 2020

ESET researchers have investigated a targeted mobile espionage campaign against the Kurdish ethnic group. This campaign has been active since at least March 2020, distributing (via dedicated Facebook profiles) two Android backdoors known as 888 RAT and SpyNote, disguised as legitimate apps. These profiles appeared to be providing Android news in Kurdish, and news for the Kurds' supporters. Some of the profiles deliberately spread additional spying apps to Facebook public groups with pro-Kurd content. Data from a download site indicates at least 1,481 downloads from URLs promoted in just a few Facebook posts.

The newly discovered Android 888 RAT has been used by the *Kasablanka* group and by BladeHawk. Both of them used alternative names to refer to the same Android RAT – LodaRAT and Gaza007 respectively.

BladeHawk Android espionage

The espionage activity reported here is directly connected to two *publicly disclosed* cases published in 2020. QiAnXin Threat Intelligence Center named the group behind these attacks BladeHawk, which we have adopted. Both campaigns were distributed via Facebook, using malware that was built with commercial, automated tools (888 RAT and SpyNote), with all samples of the malware using the same C&C servers.

Distribution

We identified six Facebook profiles as part of this BladeHawk campaign, sharing these Android spying apps. We reported these profiles to Facebook and they have all been taken down. Two of the profiles were aimed at tech users while the other four posed as Kurd supporters. All these profiles were created in 2020 and shortly after creation they started posting these fake apps. These accounts, except for one, have not posted any other content besides Android RATs masquerading as legitimate apps.

These profiles are also responsible for sharing espionage apps to Facebook public groups, most of which were supporters of Masoud Barzani, former President of the Kurdistan Region; an example can be seen in Figure 1. Altogether, the targeted groups have over 11,000 followers.

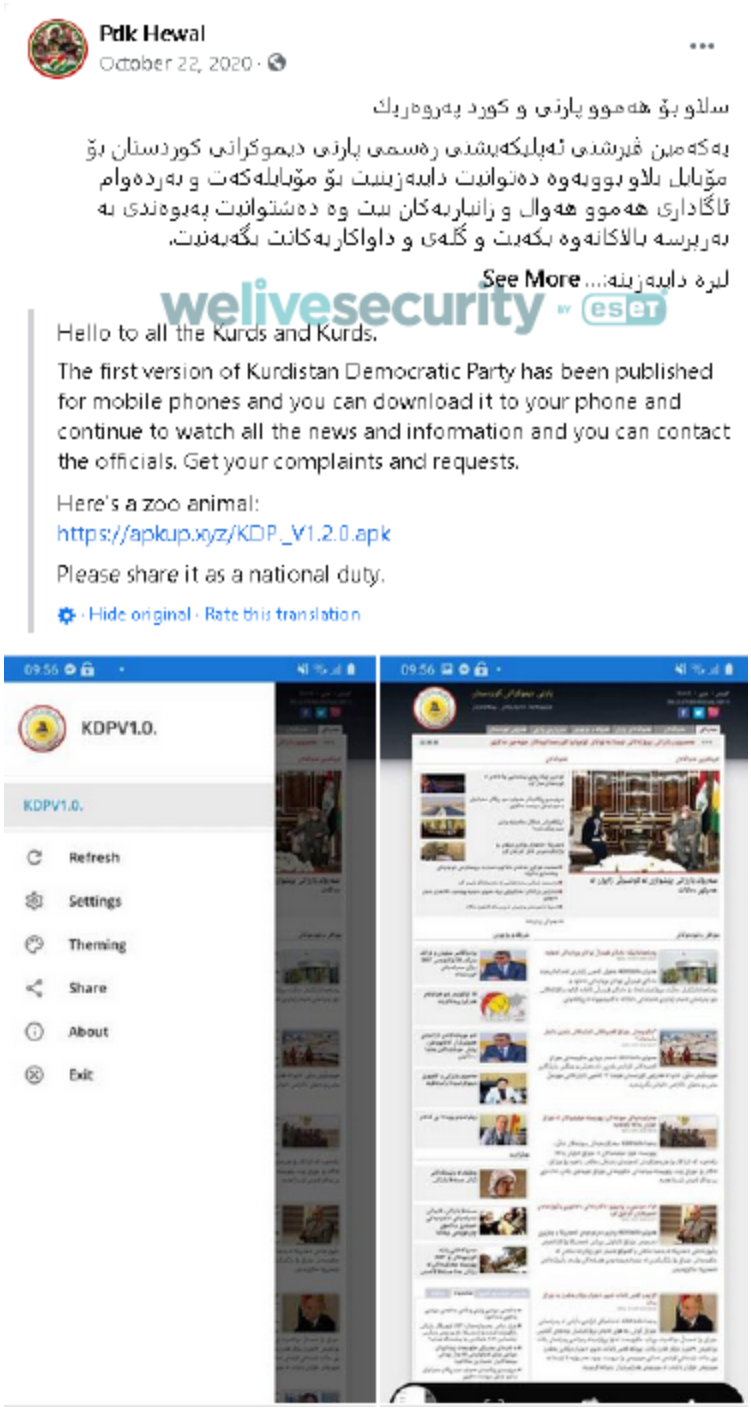

Figure 1. One of the Facebook posts

In one case, we spotted an attempt (Figure 2) to capture Snapchat credentials via a phishing website (Figure 3).

Figure 2. Facebook post leading to a Snapchat phishing site

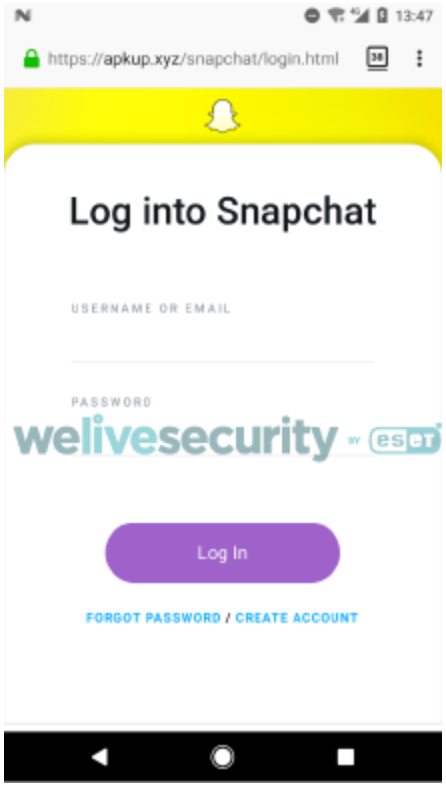

Figure 3. Snapchat phishing website

We identified 28 unique posts as part of this BladeHawk campaign. Each of these posts contained fake app descriptions and links to download an app, and we were able to download 17 unique APKs from these links. Some of the APK web links pointed directly to the malicious app, whereas others pointed to the third-party upload service top4top.io, which tracks the number of file downloads (see Figure 4). Because of that, we obtained the total number of downloads from top4top.io for those eight apps. These eight apps were downloaded altogether 1,481 times, from July 20, 2020 until June 28, 2021.

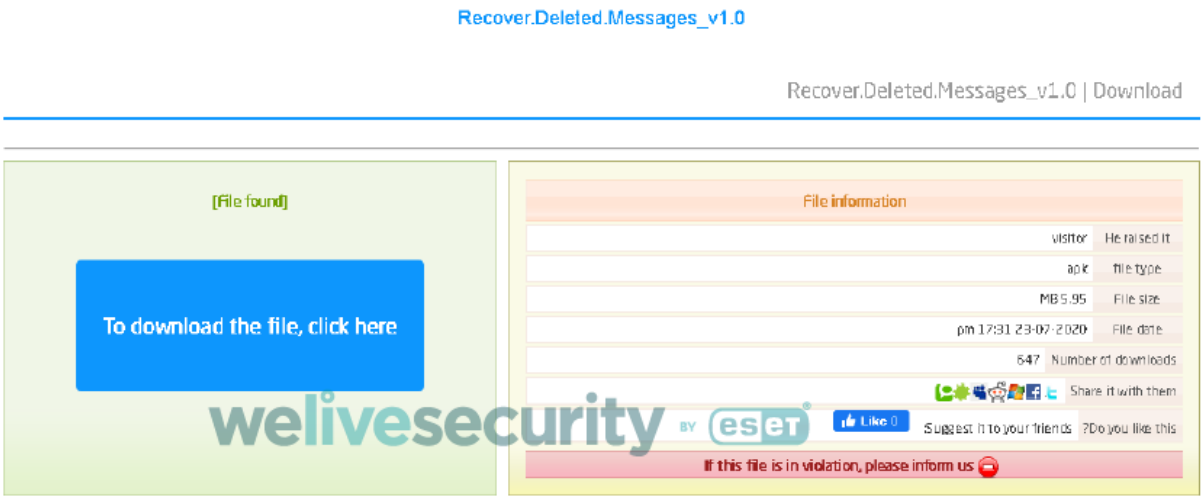

Figure 4. Information about one RAT sample hosted on a third-party service

Samples

To our knowledge, this campaign targeted only Android users, with the threat actors focused on two commercial Android RAT tools – 888 RAT and SpyNote. We found only one sample of the latter during our research. As it was built using an old, already analyzed *SpyNote builder*, here we include only the analysis of the 888 RAT samples.

Android 888 RAT

This commercial, multiplatform RAT was originally only published for the Windows ecosystem for $80. In June 2018, it was extended in the Pro version with the additional capability to build Android RATs ($150). Later, the Extreme version could create Linux payloads as well ($200).

It was sold via the developer's website at 888-tools[.]com (see Figure 5).

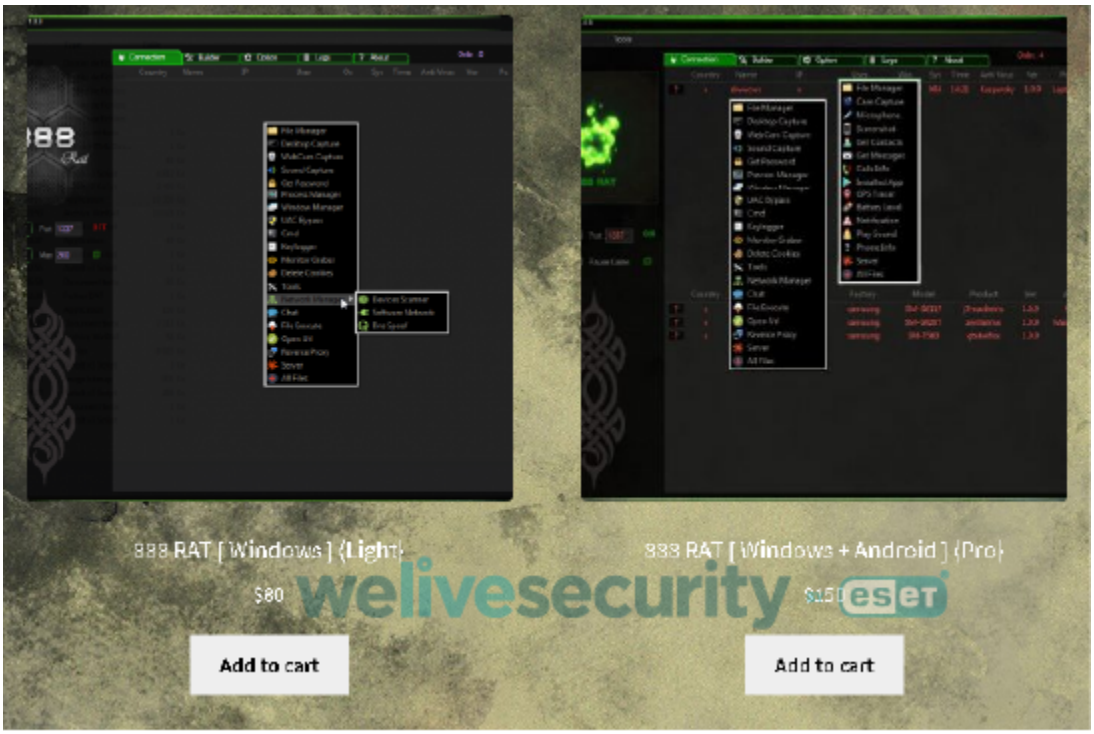

Figure 5. Price for 888 RAT

In 2019 the Pro version (Windows and Android) was found cracked (see Figure 6) and available on a few websites for free.

Figure 6. Cracked version of 888 RAT builder

888 RAT has not been directly identified with any organized campaigns before; this is the first time this RAT has been assigned as an indicator of a cyberespionage group.

Following this discovery, we were able to connect the Android 888 RAT to two more organized campaigns: Spy TikTok Pro *described here* and a campaign *by Kasablanka Group*.

Functionality

Android 888 RAT is capable of executing 42 commands received from its C&C server, as seen in Table 1.

In short, it can steal and delete files from a device, take screenshots, get device location, phish Facebook credentials, get a list of installed apps, steal user photos, take photos, record surrounding audio and phone calls, make calls, steal SMS messages, steal the device's contact list, send text messages, etc.

The builder is also used as the C&C to control all the compromised devices since it uses dynamic DNS to be reached by them.

Table 1. List of supported commands

Command	Functionality
Unistxcr	Display app details of specified app
dowsizetr	Upload file to server from /sdcard/DCIM/.dat/
DOWdeletx	Delete file from /sdcard/DCIM/.dat/
Xr7aou	Upload binary file to server from /sdcard/DCIM/.dat/
Caspylistx	List files from /sdcard/DCIM/.dat/
spxcheck	Check whether call recording service is running
S8p8y0	Stop call recording service
Sxpxy1	Enable call recording service
screXmex	Take screenshot and upload to server
Batrxiops	Get battery level
L4oclOCMAWS	Get device location
FdelSRRT	Delete file /sdcard/DCIM/.fdat (phished Facebook credentials)
chkstzeaw	Check whether Facebook app is installed
IODBSSUEEZ	Upload Facebook credentials to C&C from /sdcard/DCIM/.fdat
GUIFXB	Launch Facebook phishing activity
osEEs	Get requested permissions of the specified application
LUNAPXER	Launch specific application
Gapxplister	Get list of applications installed on the device

Command	Functionality
DOTRall8xxe	Compress files in /sdcard/DCIM/.dat/ directory and upload them to C&C
Acouxacour	Get all device accounts
Fimxmiisx	Take photo from camera and upload it to C&C
Scxreexcv4	Get information about device cameras
micmokmi8x	Record surrounding audio for the specified time
DTXXTEGE3	Delete specific file from /sdcard directory
ODDSEe	Open specific URL in default browser
Yufsssp	Get Exif information from specific media file
getsssspo	Get info about whether a specific file exists on device
DXCXIXM	Get names of all photos stored in /sdcard/DCIM/
f5iledowqqww	Upload specific file from /sdcard/ directory
GExCaalsss7	Get call logs from device
SDgex8se	List files from specific directory from /sdcard
PHOCAs7	Make call to specified number
Gxextsxms	Get SMS inbox
Msppossag	Send SMS message to specified number
Getconstactx	Get contacts
Rinxgosa	Play ringtone for six seconds
Shetermix	Execute shell command
bithsssp64	Execute shell script
Deldatall8	Cleanup, remove all /sdcard/DCIM/.dat files
pvvvoze	Get IP address
paltexw	Get TTL from PING command
M0xSSw9	Display specific Toast message to user

An important factor when identifying 888 RAT is the package name of the payload. The package name of every build of an Android payload is not custom or random; it always uses the com.example.dat.a8andoserverx package ID. Because of this, it is easy to identify such samples as 888 RAT.

In later versions of the 888 RAT (not the cracked RAT builder), we noticed that the builder was capable of obfuscating strings (command strings, C&C, and other plain text strings) by encrypting them using AES with a hardcoded key; however, the package name still remained the same.

C&C

888 RAT uses a custom IP protocol and port (it doesn't have to be standard ports). Compromised devices are controlled directly from the builder GUI.

Facebook phishing

When this functionality is triggered, 888 RAT will deploy phishing activity that appears to be coming from the legitimate Facebook app. When the user taps on the recent apps button, this activity will seem legitimate, as seen in Figure 7. However, after a long press on this app's icon, as in Figure 8, the true app name responsible for the Facebook login request is disclosed.

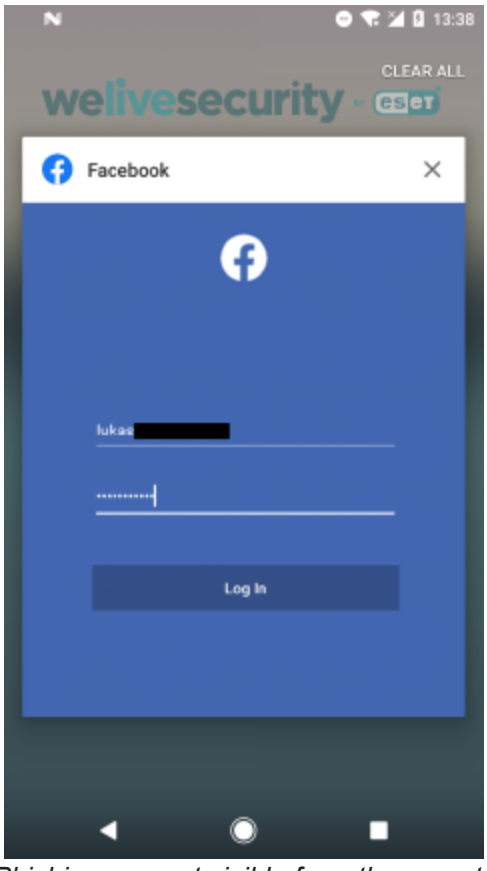

Figure 7. Phishing request visible from the recent app menu

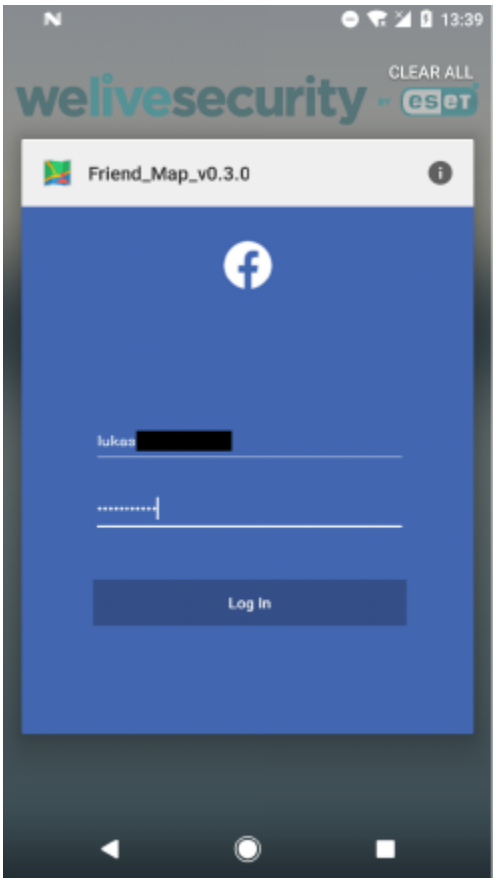

Figure 8. Real application name responsible for phishing

Detection

Since 2018, ESET products have identified hundreds of instances of Android devices where the 888 RAT was deployed. Figure 9 presents the country distribution of this detection data.

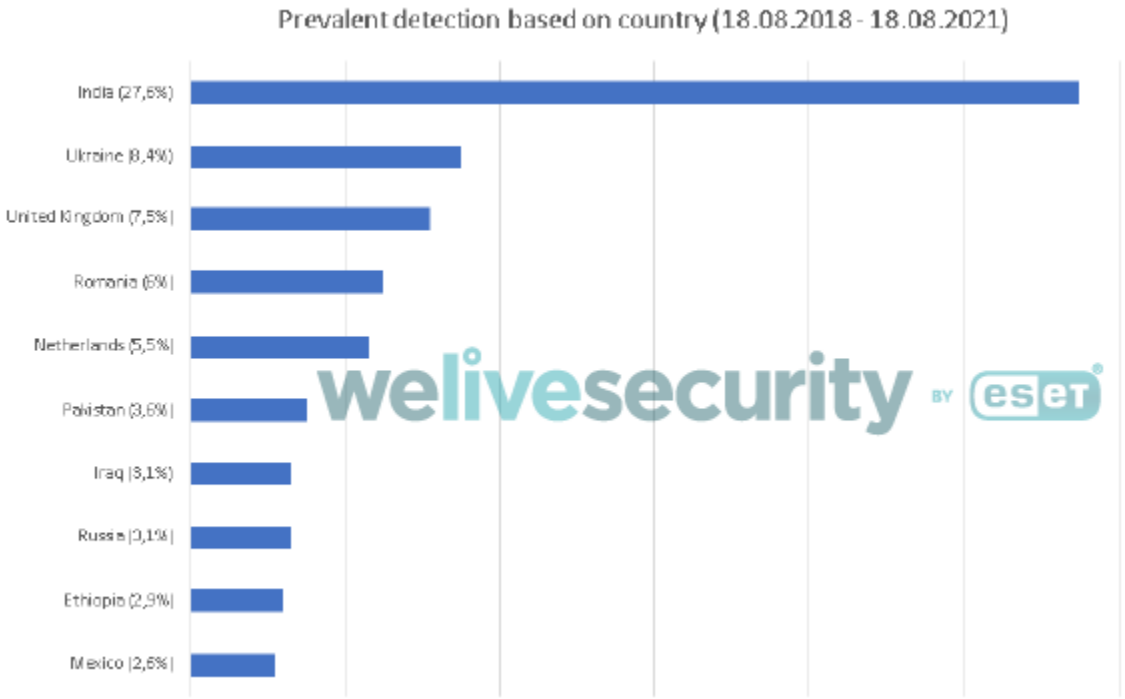

Figure 9. Detection of Android 888 RAT by country

Conclusion

This espionage campaign has been active since March 2020 aiming only at Android devices. It targeted the Kurdish ethnic group through at least 28 malicious Facebook posts that would lead potential victims to download Android 888 RAT or SpyNote. Most of the malicious Facebook posts led to downloads of the commercial, multiplatform 888 RAT, which has been available on the black market since 2018. In 2019, a cracked copy of the Pro version of the 888 RAT builder was made available from a few websites, and since then, we detected hundreds of cases all around the world using the Android 888 RAT.

IoCs

Files and ESET detection names

SHA-1	Detection name
87D44633F99A94C9B5F29F3FE75D04B2AB2508BA	Android/Spy.Agent.APU
E47AB984C0EC7872B458AAD803BE637F3EE6F3CA	Android/Spy.Agent.APG
9A8E5BAD246FC7B3D844BB434E8F697BE4A7A703	Android/Spy.Agent.APU
FED42AB6665649787C6D6164A6787B13513B4A41	Android/Spy.Agent.APU
8E2636F690CF67F44684887EB473A38398234430	Android/Spy.Agent.APU
F0751F2715BEA20A6D5CD7E9792DBA0FA45394A5	Android/Spy.Agent.APU
60280E2F6B940D5CBDC3D538E2B83751DB082F46	Android/Spy.Agent.APU
F26ADA23739366B9EBBF08BABD5000023921465C	Android/Spy.Agent.APU
4EBEED1CFAC3FE5A290FA5BF37E6C6072A6869A7	Android/Spy.Agent.APU
A15F67430000E3F6B88CD965A01239066C0D23B3	Android/Spy.Agent.BII
425AC620A0BB584D59303A62067CC6663C76A65D	Android/Spy.Agent.APU
4159E3A4BD99067A5F8025FC59473AC53E07B213	Android/Spy.Agent.APU
EF9D9BF1876270393615A21AB3917FCBE91BFC60	Android/Spy.Agent.APU
231296E505BC40FFE7D308D528A3664BFFF069E4	Android/Spy.Agent.APU
906AD75A05E4581A6D0E3984AD0E6524C235A592	Android/Spy.Agent.APU
43F36C86BBD370884E77DFD496FD918A2D9E023D	Android/Spy.Agent.APU
8B03CE129F6B1A913B6B143BB883FC79C2DF1904	Android/Spy.Agent.APU

Facebook profiles

https://www.facebook[.]com/android4kurd.official/
https://www.facebook[.]com/tech.info00
https://www.facebook[.]com/hewr.dliwar
https://www.facebook[.]com/husain.techno
https://www.facebook[.]com/zaid.abd.3785
https://www.facebook[.]com/profile.php?id=100039915424311

Facebook groups

https://www.facebook[.]com/groups/478454429578545/
https://www.facebook[.]com/groups/275108075847240/
https://www.facebook[.]com/groups/751242802375989/
https://www.facebook[.]com/groups/238330163213092/

Distribution links

https://apkup[.]xyz/M.Muhammad.Mala.Fayaq_v0.0.6.apk
https://apkup[.]xyz/5G.VPN.Speed_v1.3.4.apk
https://apkup[.]xyz/Ftwa.Islam.Online_v1.0.1.apk
https://apkup[.]xyz/Al-Hashd_V1.0.3.apk
https://apkup[.]xyz/KitabAltawhid_v1.0.4.apk
https://apkup[.]xyz/KDP._V1.2.0.apk
https://apkup[.]xyz/Dosyay16October_V1.2.0.apk
https://apkup[.]xyz/MobileNumberFinder__v1.3.apk
https://f.top4top[.]io/f_LusheAYOtmjzehyF8seQcA/1613135449/1662yvch41.apk
https://a.top4top[.]io/f_Jlno8C2DLeaq71Fq1JV6hg/1613565568/1837ppxen1.apk
https://b.top4top[.]io/f_yTmhbte0yVNbhQbKyh12og/1613135036/1665tzq3x1.apk
https://j.top4top[.]io/f_FQCcQa5qAWHzK_0NdcGWyg/1613134993/16874mc5b1.apk
https://l.top4top[.]io/f_MHfW2u_xnKoXdhjPknEx5Q/1613134914/1703t5b2z1.apk
https://b.top4top[.]io/f_cbXNkHR0T0ZOsTecrGM6iA/1613134863/1703lttbn1.apk
https://k.top4top[.]io/f_bznLRhgqMpAmWXYp1LLrNQ/1613134409/1690q040d1.apk
https://d.top4top[.]io/f_t7G4JjYm7_kzTsa0XYis6Q/1613134182/1749lglct1.apk
https://up4net[.]com/uploads/up4net-Xwakurk-1-0-4.apk

Phishing links

https://apkup[.]xyz/snapchat/login.html

MITRE ATT&CK techniques

This table only covers TTPs for 888 RAT, and was built using version 9 of the ATT&CK framework.

Tactic	ID	Name	Description
Initial Access	T1444	Masquerade as Legitimate Application	The 888 RAT impersonates legitimate applications.
Persistence	T1402	Broadcast Receivers	The 888 RAT listens for the BOOT_COMPLETED broadcast, ensuring that the app's functionality will be activated every time the device starts.
Defense Evasion	T1508	Suppress Application Icon	The 888 RAT hides its icon.
T1447	Delete Device Data	The 888 RAT can delete gathered and temporary stored files and any other specific file.	
Credential Access	T1411	Input Prompt	The 888 RAT tries to phish Facebook credentials.
Discovery	T1418	Application Discovery	The 888 RAT obtains a list of installed apps.
T1420	File and Directory Discovery	The 888 RAT identifies content of specific directories.	
Collection	T1433	Access Call Log	The 888 RAT exfiltrates call log history.
T1430	Location Tracking	The 888 RAT retrieves device location.	
T1432	Access Contact List	The 888 RAT exfiltrates the victim’s contact list.	
T1429	Capture Audio	The 888 RAT can record audio from surroundings and calls.	
T1512	Capture Camera	The 888 RAT can take pictures from the front or rear cameras.	

Tactic	ID	Name	Description
	T1412	Capture SMS Messages	The 888 RAT can exfiltrate sent and received SMS messages.
	T1533	Data from Local System	The 888 RAT exfiltrates files with particular extensions from external media.
	T1513	Screen Capture	The 888 RAT can take screenshots.
Command And Control	T1509	Uncommonly Used Port	The 888 RAT communicates with its C&C over port 4000.
Impact	T1582	SMS Control	The 888 RAT adversary can send SMS messages.
	T1447	Delete Device Data	The 888 RAT can delete attacker-specified files from the device.

7 Sep 2021 - 02:30PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion