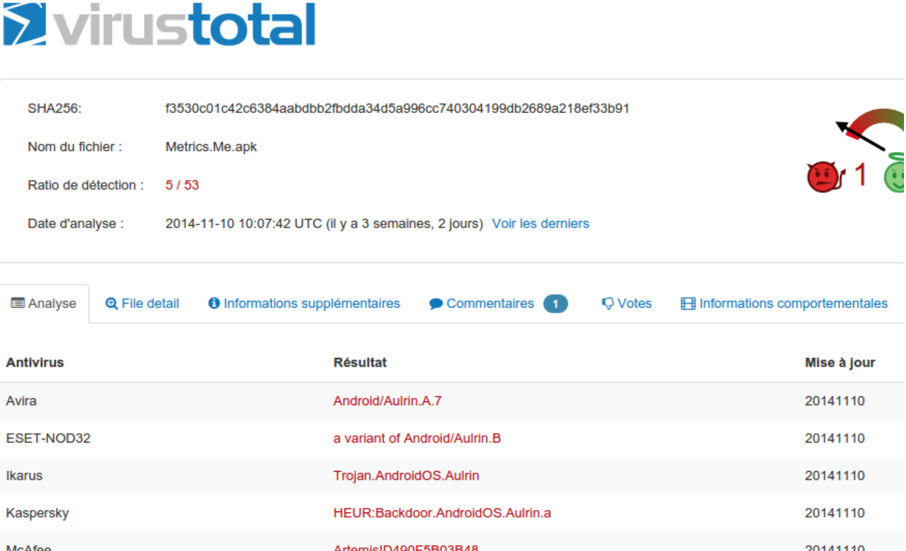
Somehow unusual Android malware sample

Łukasz Siewierski
@maldr0id

botconf
The botnet fighting conference
2014

Looking for a sample?

```
tag:apk tag:via-tor s:1
```



SHA256: f3530c01c42c6384aabdbb2fbdda34d5a996cc740304199db2689a218ef33b91

Nom du fichier : Metrics.Me.apk

Ratio de détection : 5 / 53

Date d'analyse : 2014-11-10 10:07:42 UTC (il y a 3 semaines, 2 jours) Voir les derniers

Antivirus	Résultat	Mise à jour
Avira	Android/Aulrin.A.7	20141110
ESET-NOD32	a variant of Android/Aulrin.B	20141110
Ikarus	Trojan.AndroidOS.Aulrin	20141110
Kaspersky	HEUR:Backdoor.AndroidOS.Aulrin.a	20141110
McAfee	Artemis!D490F5B03B48	20141110

Permissions

android.permission.ACCESS_FINE_LOCATION (fine (GPS) location)

android.permission.SEND_SMS (send SMS messages)

android.permission.RECEIVE_BOOT_COMPLETED (automatically start at boot)

android.permission.CONTROL_LOCATION_UPDATES (control location update notifications)

android.permission.ACCESS_MOCK_LOCATION (mock location sources for testing)

android.permission.MODIFY_PHONE_STATE (modify phone status)

android.permission.ACCESS_LOCATION_EXTRA_COMMANDS

android.permission.CHANGE_COMPONENT_ENABLED_STATE

android.permission.RECEIVE_SMS (receive SMS)

android.permission.READ_PHONE_STATE (read phone state and identity)

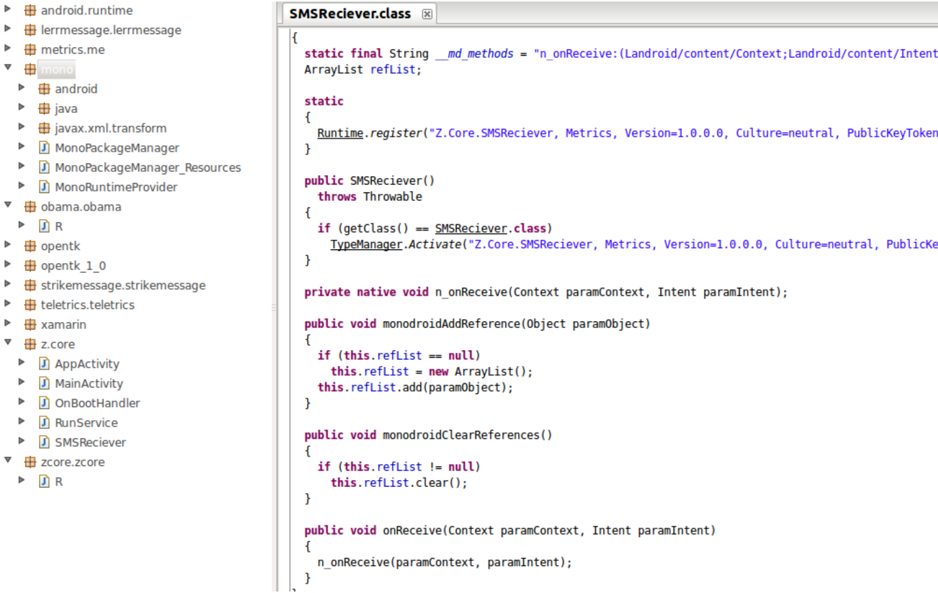
android.permission.INTERNET (full Internet access)

android.permission.WRITE_EXTERNAL_STORAGE (modify/delete SD card contents)

android.permission.READ_CONTACTS (read contact data)

android.permission.READ_SMS (read SMS or MMS)

SMS Receiver

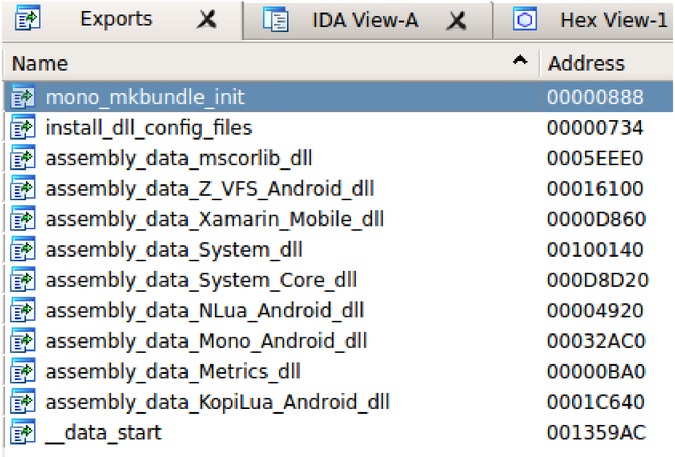


- android.runtime
- lerrmessage.lerrmessage
- metrics.me
- mono
  - android
  - java
  - javax.xml.transform
  - MonoPackageManager
  - MonoPackageManager_Resources
  - MonoRuntimeProvider
- obama.obama
  - R
- opentk
- opentk_1_0
- strikemessage.strikemessage
- teletrics.teletrics
- xamarin
- z.core
  - AppActivity
  - MainActivity
  - OnBootHandler
  - RunService
  - SMSReciever
- zcore.zcore
  - R

```
{
  static final String __md_methods = "n_onReceive:(Landroid/content/Context;Landroid/content/Intent
  ArrayList refList;

  static
  {
    Runtime.register("Z.Core.SMSReciever, Metrics, Version=1.0.0.0, Culture=neutral, PublicKeyToken
  }

  public SMSReciever()
    throws Throwable
  {
    if (getClass() == SMSReciever.class)
      TypeManager.Activate("Z.Core.SMSReciever, Metrics, Version=1.0.0.0, Culture=neutral, PublicKe
  }

  private native void n_onReceive(Context paramContext, Intent paramIntent);

  public void monodroidAddReference(Object paramObject)
  {
    if (this.refList == null)
      this.refList = new ArrayList();
    this.refList.add(paramObject);
  }

  public void monodroidClearReferences()
  {
    if (this.refList != null)
      this.refList.clear();
  }

  public void onReceive(Context paramContext, Intent paramIntent)
  {
    n_onReceive(paramContext, paramIntent);
  }
}
```

Mono? .NET?

```
samples/aulrin/lib/armeabi-v7a$ ls

libmonodroid_bundle_app.so libmonodroid.so
libmonosgen-2.0.so
```



Name	Address
mono_mkbundle_init	00000888
install_dll_config_files	00000734
assembly_data_mscorlib_dll	0005EEE0
assembly_data_Z_VFS_Android_dll	00016100
assembly_data_Xamarin_Mobile_dll	0000D860
assembly_data_System_dll	00100140
assembly_data_System_Core_dll	000D8D20
assembly_data_NLua_Android_dll	00004920
assembly_data_Mono_Android_dll	00032AC0
assembly_data_Metrics_dll	00000BA0
assembly_data_KopiLua_Android_dll	0001C640
__data_start	001359AC

Questions for you!

How to un-bundle mkbundle?

What's Lua doing there?

Sample hash: `7350decd88f7810d6b655f94abe4aac6`

You can reach me via:

🐦 @maldr0id

🅱 maldr0id.blogspot.fr