

# Lets Play Applanting...



Ajit Hatti



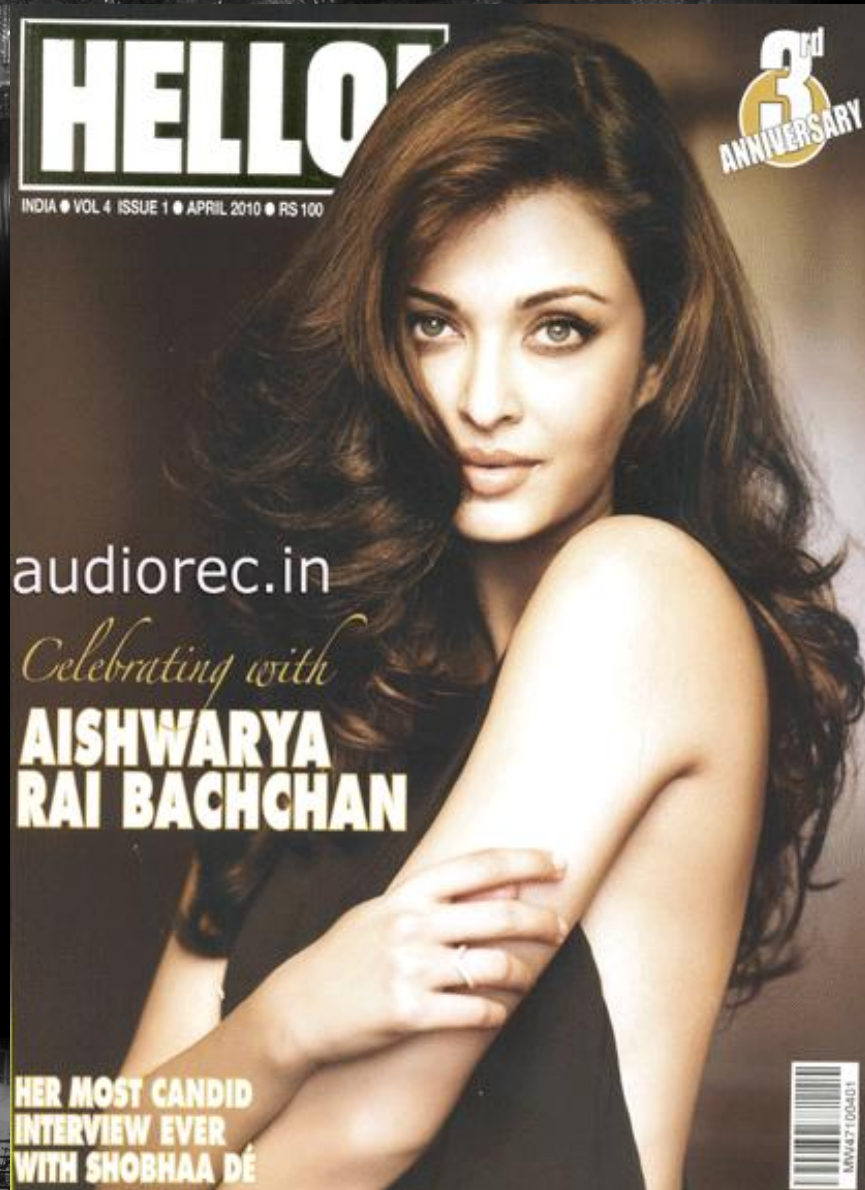
(Co-Founder)  
Null – Open Security Community





**black hat**<sup>®</sup>  
EU 2013

# HELLO From INDIA (Technically...)



# Disclaimer

Personal Research

Personal Views

Doesn't represent views of my Employer.

Vulnerabilities discussed in the paper are fixed by Google.

.

# Who Am I?

co-founder “n|u - open security community”

Working on Security of NetBackup Product family  
at Symantec

Research on Critical Information Infrastructure  
Security.





AUSTRALIAN EDITION

SECURE  
BUSINESS  
INTELLIGENCE

POPULAR: [hack](#), [mobile](#), [sec](#)

[HOME](#) [NEWS](#) [IN DEPTH](#) [REVIEWS](#) [EVENTS](#) [SC AWARDS](#)

WHAT WE'RE FOLLOWING: [RSA 2013](#) • [Carding and fraud](#) • [Jobs](#) • [Print edition](#)

[Home](#) / [Security News](#) / [Networks](#)

## Indian Govt pays bounty for botnet probe

By *Darren Pauli* on Mar 12, 2013 8:36 PM

Filed under [Networks](#)

**Text file dropped on server, but organiser says botnet was not attacked.**



7



14



2



1 Comment and 14 Reactions



A government bug bounty competition pitting white hat hackers against a live botnet has ruffled the feathers of some in the security industry.

Delegates at the [Nullcon](#) security event in Goa last month were tasked with investigating the command and control servers used in a recent attack against Indian Government infrastructure.



# The HoneyNet Project

[Home](#) > [Blogs](#) > [david.dittrich's blog](#)

## Navigation

- ◇ [About us](#)
- ▽ [Blogs](#)
  - ▷ [HoneyNet Project Blog](#)
- ◇ [Funding/Donations](#)
- ▷ [Challenges](#)
- ▷ [Chapters](#)
- ◇ [Papers](#)
- ◇ [Projects](#)
- ◇ [Code of Conduct](#)
- ▷ [Google SoC 2009](#)
- ▷ [Google SoC 2010](#)

## A new infosec era? Or a new infosec error?

Mon, 03/11/2013 - 08:54 — david.dittrich

On March 4, 2013, a contest was held at the Nullcon conference in Goa, India, to see who could take over a botnet. The Times of India reported that the prize money was provided by an Indian government official and was awarded to the Garage4Hackers team. The co-founder of the Nullcon conference, Antriksh Shah, said "At Nullcon Goa 2013, for the first time in the world the government has come forward and announced a bounty prize of Rs 35,000 to whoever provides critical information on the command and control servers of a malware recently found in one of the government installations in India," and then tweeted, "Dawn of new infosec era. Govt of India announced (and actually paid) first ever bounty (Rs. 35 k) at nullcon to take down a c&c." When asked whether this was a live botnet, or a simulated botnet held within a safe and isolated virtual network where no harm could result, Nullcon tweeted, "it was a live campaign up since a couple of yrs and the malware was found in a gov. Infra."



# Thank you, Questions ?

Can you hack Gmail/Facebook Account?

Can you hack the banks and make big money??





# Let's Play - Applanting

It involves both :

1. Hacking Gmail or a google account

&

2. Then Hack the Bank Accounts to make money

# This Paper is

About: design and gap in Google's Play store along with few XSS vulnerabilities discovered in late last year.

Aimed : To create awareness about an interesting attack possibility called Applanting.

Not Claims : success of the attack as Google has been very fast and better in fixing the security issues in their services

Definetely Claims : Similar attacks in future on platform other than Android

# Motivations

<http://nullcon.net>

nju **CON**

**How Secure is  
Internet Banking  
in INDIA?**



**Ajit Hatti**

[ajit.hatti.sec@gmail.com](mailto:ajit.hatti.sec@gmail.com)

nullcon

International Security Conference

delhi 2012

# Bank Identifies you by your Phone

|  |   |  |  |
|--|---|--|--|
| <br>ABN AMRO BANK                   | <br>AXIS BANK        | <br>BANK OF INDIA           | <br>BANK OF PUNJAB        |
| <br>CITIBANK BANK<br>ACCOUNT ONLINE | <br>CORPORATION BANK | <br>FEDERAL BANK            | <br>HDFC DIRECT PAY        |
| <br>ICICI BANK                      | <br>IDBI BANK        | <br>PUNJAB<br>NATIONAL BANK | <br>STATE BANK OF<br>INDIA |
| <br>UNION BANK<br>OF INDIA         | <br>YES BANK        | and many more.   |  |



# Reliable and Cheaper alternative



|                   |                              |
|-------------------|------------------------------|
| Debit Account     | 861-123-456789-0 HKD Current |
| Withdrawal Amount | HKD 15,000.00                |
| To                | 861-123-987654-9             |
| Transfer Amount   | HKD 15,000.00                |
| Exchange Rate     | N/A                          |
| Transfer On       | 31-OCT-2010                  |
| Template remarks  |                              |

Please authenticate to confirm the transaction

Mobile Phone: 91234567  
SMS Reference: 000001  
One Time Password:

31/10/2010  
06:22 pm

ICBC(ASIA)  
FUND TRANSFER  
A/C NO. \*\*\*\*\*-789-0  
HKD15,000.00  
SMS REF. 000001  
PIN:1234ABCD

A red arrow points from the PIN field in the mobile phone screen to the One Time Password field in the transaction confirmation screen.

# The Concern

Your Phone Is your Identity

# Facebook Identifies you by your Phone

&

So dose Google services...



# Your Phone Is your Identity

*Mom, The man at the door says he is my dad, and his Mobile number is saved in your cell phone as "Rascal", should I open the door?*





# Motivations



Lt. Col MS Dhoni, Planting Campaign



# The Play Ground

https://play.google.com/store/apps/details?id=com.nullcon.android&feature=search\_result#?t=W251bGwsMSwyLDEsImNvb55u ☆ ↻ ↻ Google

Search Images Maps **Play** YouTube News Gmail More ▾

Google play Search

SHOP ANDROID APPS MY ANDROID APPS

**NullCon Delhi 2012**  
nullcon



★★★★★ (3)

INSTALL

**This app is compatible with your**  
IDEA Motorola MB525.

Users who viewed this also viewed



**Mobile AntiVirus Security P...**  
AVG MOBILE TECHNOLOGIES  
★★★★★ (7,928)  
Rs.1,095.00



**Google Apps Device Policy**  
GOOGLE INC. ↕  
★★★★★ (1,831)  
Free

**OVERVIEW** USER REVIEWS WHAT'S NEW PERMISSIONS

### Description

Nullcon Delhi, brings together CXOs, Security Researchers, IT Professionals and Senior Management in a collaborative environment to present and discuss issues relating to IT security. The conference would be attended by eminent representatives of the Information Security domain, leaders of large and small enterprises, senior Government officials, policy and decision makers from around the globe.

[Visit Developer's Website](#) > [Email Developer](#) >

### App Screenshots



g+1 2  
Tweet

### ABOUT THIS APP

RATING:  
★★★★★  
(3)

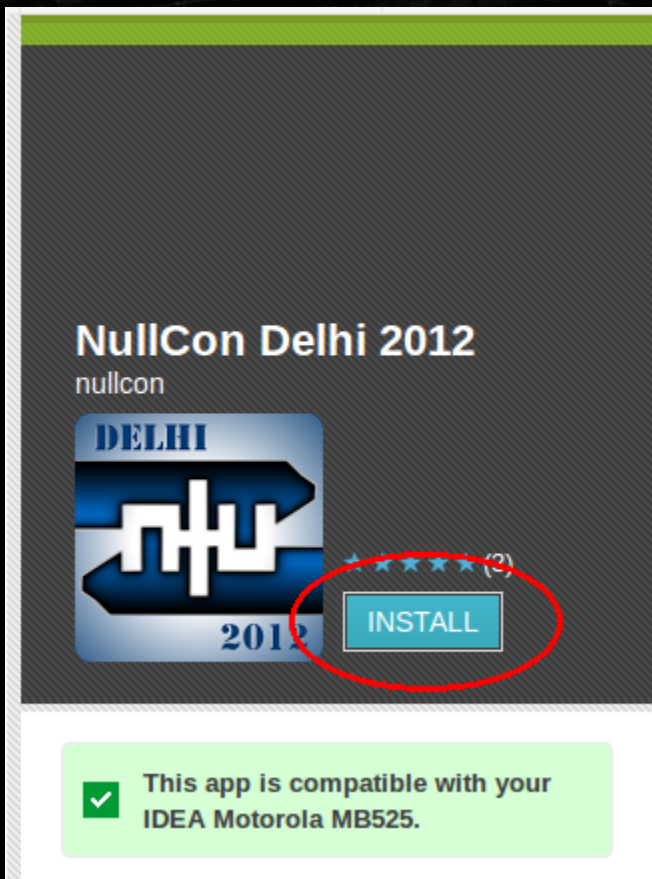
UPDATED:  
July 25, 2012

CURRENT VERSION:  
1.0.0

REQUIRES ANDROID:  
2.1 - 2.3.7

CATEGORY:  
Communication

# The Rules



NullCon Delhi 2012  
nullcon

DELHI  
NHU  
2012

INSTALL

✓ This app is compatible with your  
IDEA Motorola MB525.

```
POST /store/install HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded;charset=utf-8
Referer: https://play.google.com/store/apps/details?
id=com.nullcon.android&feature=search_result
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64;
Trident/6.0)
Host: play.google.com
Content-Length: 139
DNT: 1
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: __utma=45884901.1454077777.1354703478.1354703478.1354710207.2;
__utmb=45884901.5.10.1354710207; __utmz=45884901.1354703478.1.1.utmcsr=
(direct)|utmccn=(direct)|utmcmd=(none); __utmc=45884901; hlSession2=en;
PREF=ID=039ba4488bbc7e93:U=539a9f5e8e30448b:FF=0:LD=te:TM=1353568374:LM=13547
NID=66=thFWPFdFuXsSMYn2i8Jk11GJAF LX6LtoXUJhAD_isXFg1jN6-2atIzvbmb6LqIQgjsyWRNE
j42qYqmRkJdYlPeve67XBnXAFjoAXFDVowbjBtd8Lqa86vY59KQ;
GMAIL_LOGIN=T1354698419824/1354698419824/1354698436034;
SID=DQAAAMIAAAARgFboHT3Fv_FMC0TgaK908IdzBMTALZR87zLuyL9uQjxCiJgfr6yI0USHQWvrz
Kqda4zItUmF04Yb3qWziWBqHqTlg76i20D0orA0egHrHym5E_oeumKYnfsmKmdZWJoYcoDulPs6Dv
HSID=Az1w5eyNQI5E6jNP; SSID=AxxxSaCnrF9iEV1P; APISID=Wcvdn7UmMBDXG0BB/
A2WmLP3Z492w5oEYC; SAPISID=1fL09LTnuC6XTt2Y/AILf9HURq8lqgXg60

id=com.nullcon.android&offerType=1&device=g2ed6a8be00731246&feature=search_re
%3A1354698436000|
```

# Between the lines

id=com.nullcon.android&  
offerType=1&  
device=g2ed6a8be00731246&  
xhr=1&  
token=QRnhw2PHSRv6icuuUn1z9wyEI\_U%3A1354698436000



Possible Moves:

Steal the Cookie and then.....

# Possible Moves:

```
javascript:alert(initProps['userEmail'] + ' | ' + initProps['token'] + ' | ' + initProps['selectedDeviceId'])
```

POST /store/install HTTP/1.1

Host: play.google.com

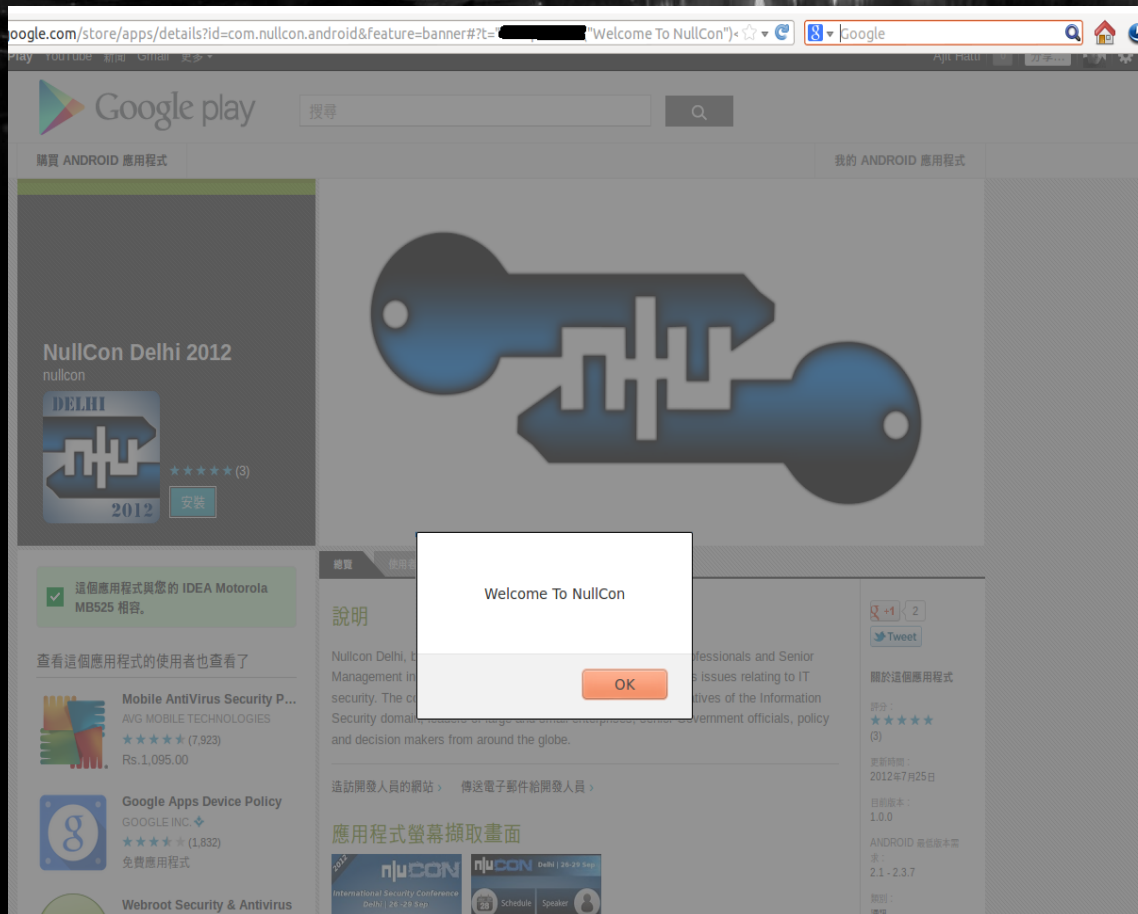
Cookie: \_\_utma=<cookie from XSS>

Content-Type: application/x-www-form-urlencoded;charset=utf-8

Content-Length: 139

id=com.company.app\_name&device=<19 digit phone ID>&xhr=1&token=<41 char token>

# The Flaw



# Possible Moves?

```
Javascript: document.getElementById('Install').click();
```

OR

```
$("#a").click(); //by tag.
```

```
$("#a[href='#']").click(); //by tag with href property
```

```
$(".side_link").click(); //by class
```

```
$("#div#someId a.side_link").click();
```

// This would work if the link was a child of a div with Id = someId



# The Goal

Google play Search

SHOP ANDROID APPS

**NullCon Delhi 2012**  
nullcon

 **2012** ★★★★★ (3) **INSTALLED**

✓ This app is compatible with your **IDEA Motorola MB525**.

Users who viewed this also viewed

-  **Mobile AntiVirus Security ...**  
AVG MOBILE TECHNOLOGIES  
★★★★★ (7,928)  
Rs.1,095.00
- Google Apps Device Policy

**OVERVIEW** USER REVIEWS WHAT'S NEW PERMISS

### Description

Nullcon Delhi, brings together CXOs, Security Researchers, IT Pro Management in a collaborative environment to present and discuss security. The conference would be attended by eminent representatives in the Security domain, leaders of large and small enterprises, senior policy and decision makers from around the globe.

[Visit Developer's Website >](#) [Email Developer >](#)

# Getting the Player to the Ground

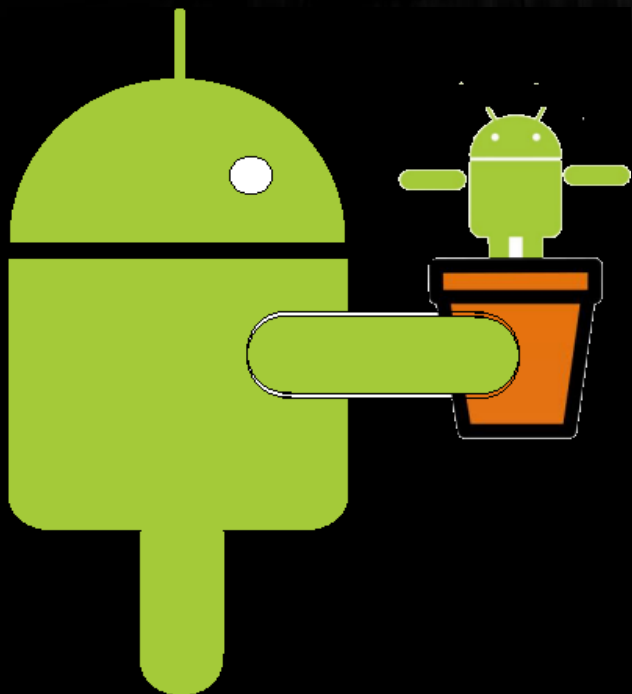
The screenshot shows a Gmail interface with a dark wood-grain theme. At the top, the Gmail logo is on the left, and navigation icons (back, forward, search, trash, move to inbox, etc.) are on the right. Below the navigation bar, a search bar contains the text "TaxACT.com - TaxACT@: Free Means Free - Free - It's How We ACT. Free to Prepare, Print and eFile IRS Taxes. E-file Now for a Fast Refund." To the left of the main content area is a sidebar with folders: "COMPOSE", "Inbox (3,469)", "Important", "Sent Mail", "Drafts (95)", "Circles", "Finance", "HEV (4)", "Personal", and "Receipts (1)". The main content area displays an email titled "New Pictures Posted" from a redacted sender to "evadermusttry" at 12:00 AM. The email body says: "Hello Evader, We have posted new pics on our site. Chekc them out : [http://null.co.in/section/events/meets/](\"http://null.co.in/section/events/meets/\")". Below the email is a "Click here to Reply or Forward" button. On the right side of the email, there is a profile for "evadermusttry" with an "Add to circles" button and a "Show details" link. Below the email, there are two advertisements: "ICICI Bank Debit Card" and "TaxACT.com: Free Means Free". The bottom of the screenshot shows the URL "null.co.in/section/events/meets/" in the address bar.

# The Action

The screenshot shows a Mozilla Firefox browser window with the following elements:

- Address Bar:** Contains the URL `null.co.in/section/1/meets/`. A red circle with the number **1** highlights the URL.
- Navigation Menu:** Includes links for HOME, JOBS, BLOG, ATHENEUM, and EVENTS. A red circle with the number **2** highlights the 'Meets' link.
- App Listing:** A Google Play store overlay for the 'NullCon Delhi 2012 - Android' app is shown. A red circle with the number **3** highlights the app listing.
- Website Content:** The main content area features the 'nju' logo and the text 'Meets'. Below this, there is a section for 'null Chennai Chapter January 2013 Meet - 2 Solutions'.

# What We Can do?



## SMS Forwarder

YASMANI / TOOLS

★★★★★ (324)

INSTALL



## SMS Forwarder

KAAN YAMANYAR / COMMUNICATION

★★★★★ (63)

INSTALL



## Auto SMS (Autoresponder)

THEIN MIN NAING / COMMUNICATION

★★★★★ (2,937)

INSTALL

# What We Can Gain?

**SMS Forwarder**  
YASMANI / TOOLS  
★★★★★ (324)  
INSTALL

**SMS Forwarder**  
KAAN YAMANYAR /  
★★★★★ (63)  
INSTALL

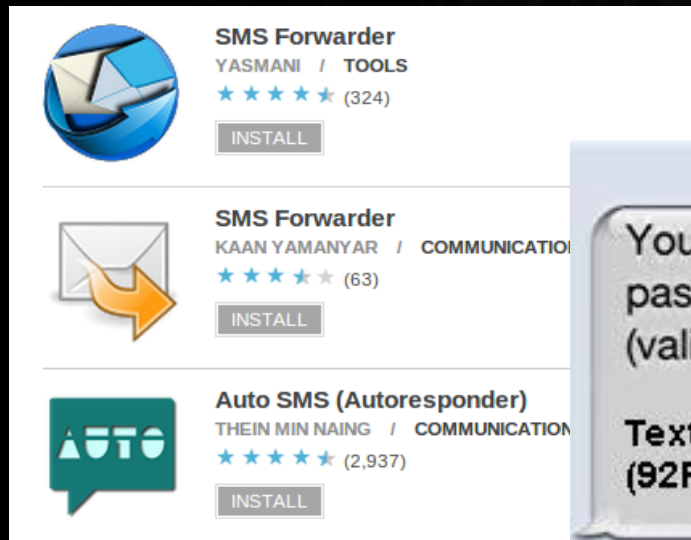
**Auto SMS (Autore)**  
THEIN MIN NAING /  
★★★★★ (2,937)  
INSTALL

Messages +65 98163299

Fr: DBS ec-banking-Increase daily limit of fund transfer to 100000.00, Tran Ref: 1234567890, please use this One Time Password (OTP):FAAW-64356501. Thank you.

|                                  |                      |                          |                         |
|----------------------------------|----------------------|--------------------------|-------------------------|
| <br>ABN AMRO BANK                | <br>AXIS BANK        | <br>BANK OF INDIA        | <br>BANK OF PUNJAB      |
| <br>CITIBANK BANK ACCOUNT ONLINE | <br>CORPORATION BANK | <br>FEDERAL BANK         | <br>HDFC DIRECT PAY     |
| <br>ICICI BANK                   | <br>IDBI BANK        | <br>PUNJAB NATIONAL BANK | <br>STATE BANK OF INDIA |
| <br>UNION BANK OF INDIA          | <br>YES BANK         | and many more.           |                         |

# What We Can Gain?



**SMS Forwarder**  
YASMANI / TOOLS  
★★★★★ (324)  
INSTALL

**SMS Forwarder**  
KAAN YAMANYAR / COMMUNICATION  
★★★★★ (63)  
INSTALL

**Auto SMS (Autoresponder)**  
THEIN MIN NAING / COMMUNICATION  
★★★★★ (2,937)  
INSTALL



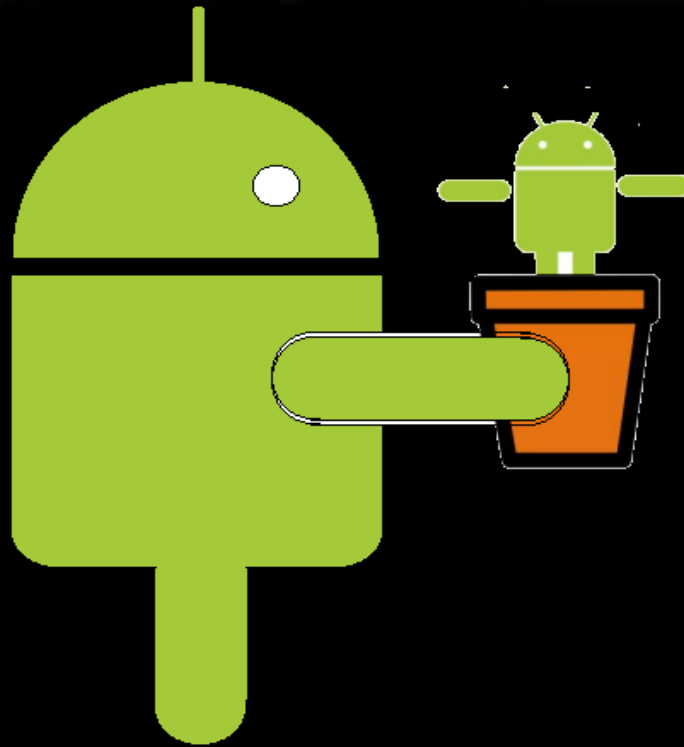
Your Facebook One-time password is tgMhztXd (valid for 20 min)

Text your status to 923223: (92FACEBOOK) to update.

Q W E R T Y

Social media sharing icons: Facebook, YouTube, Blogger, Plus, Instagram, Twitter, Messenger, Yahoo!, SoundCloud, Google, LinkedIn, QR code, Dribbble, and a group icon.

# Demonstration



# Big Thanks To

Jon Oberheide (<http://jon.oberheide.org/>)

Thomas Cannon (<http://thomascannon.net/>)

Google



# Future of Applanting

Man in mobile – very powerful exploitation Vector

Applanting is about to start grow and be a Challenge

The Challenge : As a third party, you cant differentiate between App installation by Choice or by Force



# Future of Applanting

Applanting on Windows 8 based phones

App-Forking -



# Conclusion

Concerns : Mobile is your strongest Identity & single point to screw your life.

Applanting : Flaws in App stores can be leveraged to install applications Silently.

Challenge : Cant differentiate between user chosen application installation and Applanting.

Awareness : Make sure you did installed that app on your mobile.



# Thank you All



&  
Also  
BIG Thanks to  
Team Black Hat



Lt. Col MS Dhoni,  
(Inspiring India)

Vivek Ramchandran

nullcon & Jailbreak team