SMART PHONE THREATS & COUNTER MEASURES

DISCLAIMER

This document does not promote or encourage any Illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.

TABLE OF CONTENTS

INTRODUCTION TO SMART PHONE THREATS

Analysis and assessment related to threats that really exists in real world scenarios

TRADITIONAL VS LATEST THREATS

Emulating traditional and latest threats by demonstrating different scenarios.

TRADITIONAL ATTACK & MALWARE BINDING DEMO

Binding malware with a legitimate application hosted over various open market places.

THREATS IGNORED BY A REGULAR SMARTPHONE USER

Threats associated with the highly portable devices which can impair sensitive information in the Smart phone.

INTRODUCTION TO SMART PHONE THREATS

Statistics of smart phone Users in Pakistan

Date	Android	iOS	Unknown	Nokia Unknown	Series 40	Windows	Symbian OS	BlackBerry OS	Samsung	LG	Linux	Other
2018-11	90.15	4.29	1.11	2.01	1.16	0.57	0.47	0.07	0.08	0.01	0.04	0.02
2018-12	91.17	4.13	0.87	1.73	0.97	0.53	0.41	0.06	0.07	0	0.04	0.03
2019-01	91.47	4.04	0.78	1.71	0.96	0.47	0.38	0.05	0.07	0.01	0.03	0.02

Reference: http://gs.statcounter.com/os-market-share/mobile/pakistan

Introduction to smart phone threats

Ubaid Jafri

Smart phones horizon increases after the year 2010. and at current stage there are more smart phones then PC's in the market today , and they are the most connected devices we carry today.

Damages

Accessing User Privacy

Intentionally penetrated into the smart phone and access user (Contacts, SMS, Call Logs. Videos, Pictures, Storage, etc)

Tracking Location

Tracking user current location and IP address along with Local network details

Recoding Conversation during roaming

By intruding into user cell phone, one may be able to record microphone even if the cell phone is not being used or locked

Stealing Sensitive Info

Activity would allow an attacker to steal sensitive information from cell phone e.g. (OTP, username/passwords, logged in user credentials,

Breaking Into Network

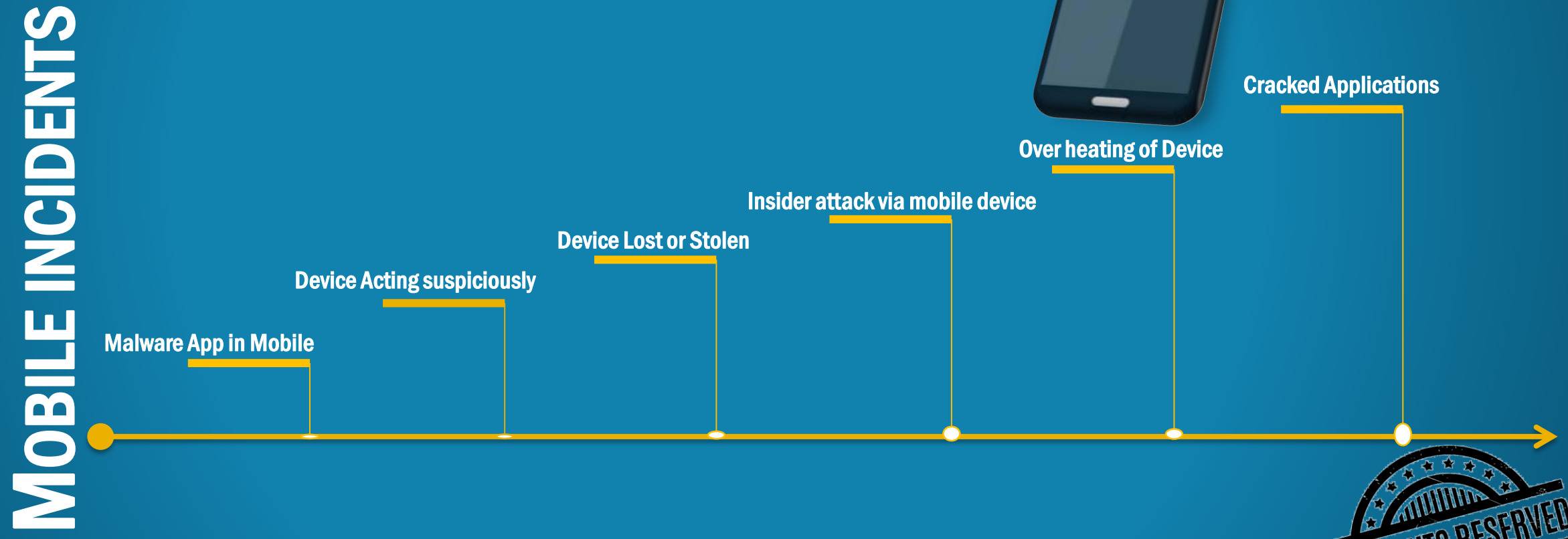
Accessing Interconnected nearby devices, exploiting network devices.

Intercepting Text Messages

Ability to send SMS from the cell phone in case of devices compromised.

Introduction to smart phone threats – Common Mobile Incidents

There are numbers of possible scenarios a user may encounter when responding to a mobile incident.

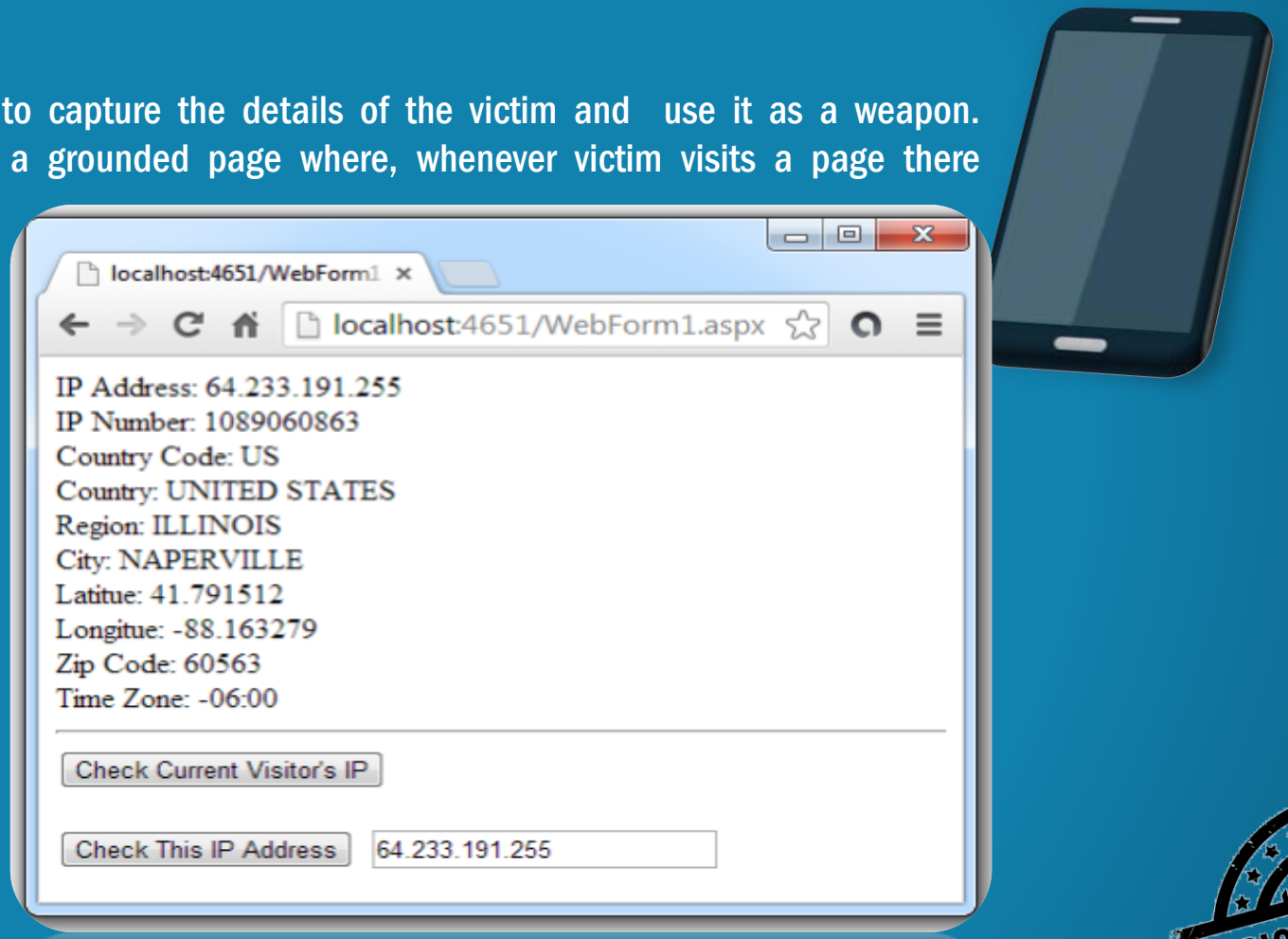


TRADITIONAL VS LATEST THREATS

TRADITIONAL VS LATEST THREATS

Traditional Threat

Unlikely traditional threats were used to capture the details of the victim and use it as a weapon. Traditional threats could be a simple a grounded page where, whenever victim visits a page there information stored in a text file or email.

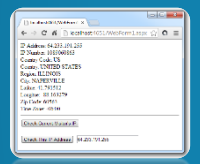


Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

DEMONSTRATION OF TRADITIONAL SMART PHONE ATTACK

Traditional Attack Demonstration

Crafting a malicious web link for victim &
Hiding actual link with URL shorteners



Send the Malicious link
using different channels

Malicious Link Will Instantly Fetch:

- ✓ Public IP Address of the victim
- ✓ Device Model
- ✓ Version Information
- ✓ Cell Phone Current Location

DEMONSTRATION OF
MALWARE BINDING

Demonstration Of Latest Cyber Attack

Binding malware with a legitimate application hosted over various open market places.

Send the Malicious link

Malicious App Contains:

- ✓ Reverse Back Connection
- ✓ Intruder IP
- ✓ Intruder Port

Malicious App Will Intrude:

- ✓ SMS (Dump, Send/Receive), Call Log, Gallery, Camera, Mic, Contact Directory, Location Tracking, File Uploading, etc

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

THREATS IGNORED BY A REGULAR SMARTPHONE USER

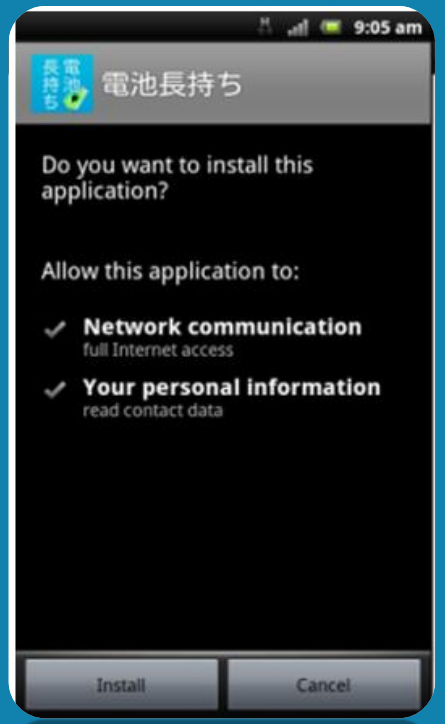
THREATS IGNORED BY A REGULAR SMARTPHONE USER

- **Third-Party Applications:**
  - ✓ Never download applications from third-party forums like:
    - ➢ PureAPKs
    - ➢ BlackMart
    - ➢ FreeAPKs, etc
  - ✓ Although these forums provide the feasibility to download applications for free but the integrity of many of these applications is affected, which can lead to breach of sensitive data.
- **Malicious Links:**
  - ✓ Never click / tap on any links received via emails or social media forums. Malicious links include:
    - ➢ http://ow.ly/d9AV30jRJWJ
    - ➢ tinyurl.com/y6wzdc4q
    - ➢ bit.ly/2xTleYF
  - ✓ These links redirect the user to malicious websites resulting in users to download the virus file and then affecting the victim's user.
- **Storage Password in Third-Party Apps:**
  - ✓ Never store passwords in third-party applications as these applications can store the sensitive data without any protection.
- **Social Engineering Attacks:**
  - ✓ Never access any link advertised as providing free products in form of offers / coupons.

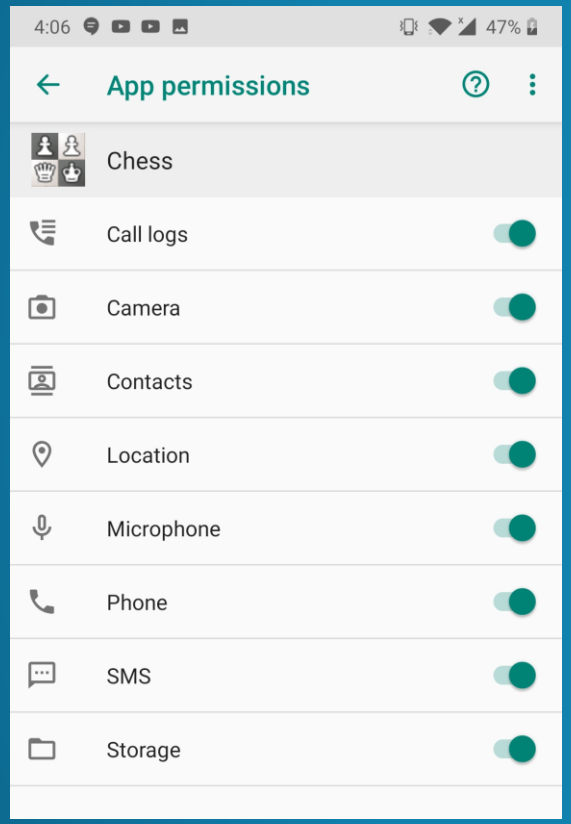
Threats ignored by a regular smartphone user Contd..

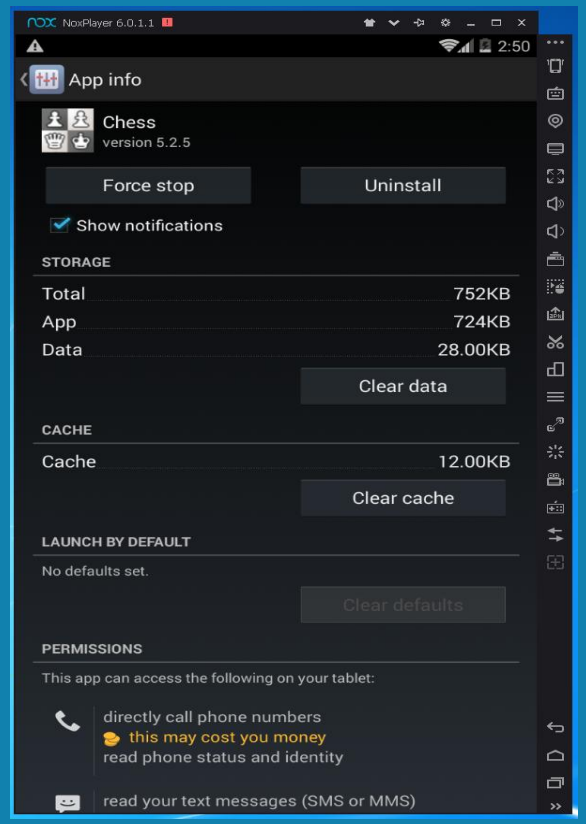
- **Downloading Fake Applications:**

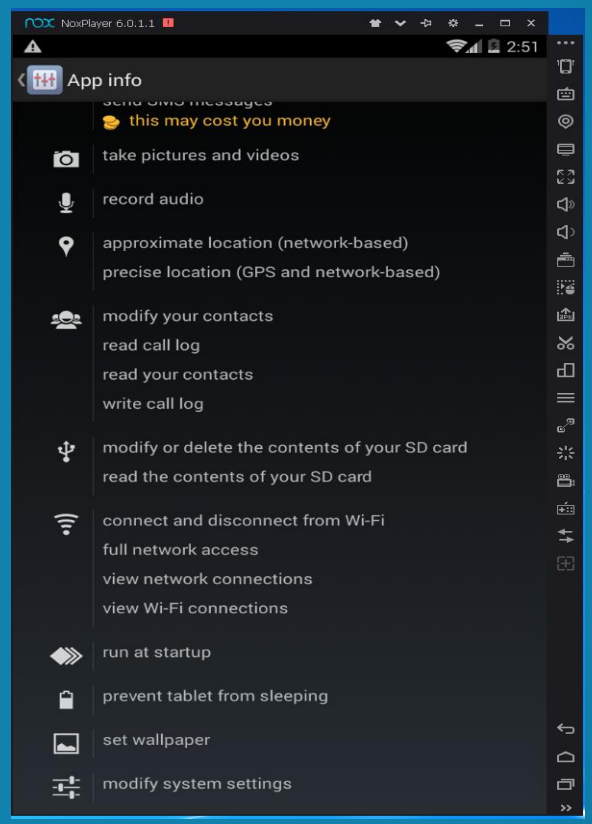
  ✓ Fake applications like battery saver pose to be helping users improving their battery performance. However these applications have malware bind with them and are causing the data leakage from smartphones.



Threats ignored by a regular smartphone user Contd..







Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

THANK YOU