Building Your Own Open-source Android Penetration Testing Platform

Amadeus Konopko
amadeuskonopko@gmail.com

JP Mitri
jpmitri@gmail.com
Disclaimer

We are not responsible for anything you do with this information or these tools. This is intended for learning purposes.
Graduated Seneca College in May 2017 from informatics and security degree program
Toward the end of the program focused heavily on Android mobile devices
Researched mobile vulnerabilities, exploits and phishing
Started working with Kali Linux and Metasploit, testing what was available to us …
Overview

• **Android:**
  - Growth, Attack Surface, Permissions and Malware

• **Attacks:**
  - Existing Tools, Attack Mediums & Platforms

• **Starphish**

• **Demo**
Android
Android Growth Spurt

Android phones since last year have risen to 86% market share

Emerging markets introduce new affordable phones driving the market share

Sources: http://www.nasdaq.com/article/the-evolution-of-smartphone-markets-where-growth-is-going-cm619105
Android Attack Surface

Application
  Broadcast Receivers, Services, Content Providers, Activities

Baseband
  Cellular Voice and Data, SMS and Radio Interface Layer (RIL)

WIFI
  PHY, MAC, MLME

Sources: https://threatpost.com/how-google-shrank-the-android-attack-surface/127086/
https://source.android.com/images/android_framework_details.png
Android Permissions

Permissions-based Security Model

Intra-library Collusion (ILC)

Protection Level Downgrade
Android Malware

Android Malware

What is it?

- Malicious code through app installation
- Existing app downloading a malicious update
- Attacker injecting malicious code
- Botnets, Rootkits, SPAM, Identity Theft, Banking Trojans, DDOS, Ad-Click, FakeAV, Ransomware, Spyware...

Source: https://www.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf
Android Malware

What does it do?

- Targeted social engineering gets user to click or install
- Malicious code runs on device
- Installs code or modifies files to achieve privilege escalations and persistence
- Takes control from a remote C2 server
- Access SMS, Email, microphone, camera, storage anytime
Android Malware

Phishing

25,000 tool used for phishing and keylogging.

12 million credentials stolen via phishing

Phishing poses the greatest threat to users next to keyloggers and third-party breaches

Source: https://security.googleblog.com/
Domain / Certificate Abuse

15,270 SSL certs containing the word “PayPal”

14,766 were phishing sites

Not preventing or taking responsibility

<table>
<thead>
<tr>
<th>Month</th>
<th># of Certs Issued</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2016</td>
<td>10</td>
</tr>
<tr>
<td>April 2016</td>
<td>57</td>
</tr>
<tr>
<td>May 2016</td>
<td>73</td>
</tr>
<tr>
<td>June 2016</td>
<td>65</td>
</tr>
<tr>
<td>July 2016</td>
<td>149</td>
</tr>
<tr>
<td>August 2016</td>
<td>231</td>
</tr>
<tr>
<td>September 2016</td>
<td>299</td>
</tr>
<tr>
<td>October 2016</td>
<td>536</td>
</tr>
<tr>
<td>November 2016</td>
<td>1276</td>
</tr>
<tr>
<td>December 2016</td>
<td>2530</td>
</tr>
<tr>
<td>January 2017</td>
<td>3995</td>
</tr>
<tr>
<td>February 2017</td>
<td>5101</td>
</tr>
</tbody>
</table>

Source: https://www.thessslstore.com/blog/lets-encrypt-phishing/
Android Remote Control

Android Remote Control

Spyware, Malware and Metasploit

Steals users text messages, emails, calls, photos, location and other data

Thousands of these apps on the Play Store

Metasploit makes it easier for an attacker to create and distribute custom malware

Sources: https://forensics.spreitzenbarth.de/android-malware/
https://blog.lookout.com/sonicspy-spyware-threat-technical-research
### Attack Mediums

<table>
<thead>
<tr>
<th>Medium</th>
<th>Tested Keys</th>
<th>Got IVs</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSM</td>
<td>1514</td>
<td>30566</td>
</tr>
<tr>
<td>USB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WIFI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bluetooth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NFC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Log:**

```
[00:00:18] Tested 1514 keys (got 30566 IVs)
```

**Output:**

```
KEY FOUND! [ 1F:1F:1F:1F:1F ]
Decrypted correctly: 100%
```
Attack Mediums

Attacking GSM/Telephony

SMS/MMS/WAP

Signaling System No. 7 (SS7)

Stingray/Surveillance/IMSI Catcher

Attack Mediums

Attacking USB

USBSwitcher

ADB

Pork Explosion

Source: https://github.com/ud2/advisories/tree/master/android/samsung/nocve-2016-0004
http://bbqand0days.com/Pork-Explosion-Unleashed/
Attack Mediums

Wifi Attacks

- KRACKs
- Evil Twin AP & Captive Portal
- Broadpwn

Source:
- https://www.krackattacks.com/
Attack Mediums

Bluetooth Attacks

BlueBorne
Bluejacking/Bluesnarfing/BlueBugging
DOS

Attack Mediums

NFC Attacks

- Eavesdropping
- Data Modification
- Relay Attack

https://www.intechopen.com/source/html/44973/media/image2.png
Platforms

Source: https://pctechmag.com/wp-content/uploads/2013/02/opens.jpg
Established

Metasploit Framework
Smartphone Pen-Test Framework / Dagah
Drozer

What we were in search of

Open-Source, Automation, Evasion, Availability and Scalability....

Source: https://www.metasploit.com/
Starphish
Starphish

What is it?

Open-Source platform that can create, modify, deploy and manage exploits and attacks for Android based devices.

It leverages the Metasploit framework for a fully featured Pen-Test suite

Can operate on multiple hardware platforms from SoC to Cloud
Starphish

Architecture

Kali Linux

Metasploit framework, payloads and rpcd

pymetasploit by allfro

king-phisher

ClockworkSMS

Source: https://kadk.dk/sites/default/files/styles/media/public/2013-14_lukaszwlodarczyk_membranestudy_cita_blog_0.jpg?itok=Ld-MNCNs&c=e639107c8fe2d0311850f61170264dc9
Starphish

Create

Using our Malware-Builder script
Pulls Metasploit payloads from Github
Implements simple anti-virus evasion
We use our own X.509 certificate to sign APKs

Starphish

Modify

The name of the malware to suit your campaign

The landing page

Phishing messages

Sources: http://www.eweek.com/imagesvr_ez/b2bezpz/2016/08/290x195blueboxfakeid1_2.jpg?alias=article_hero
Starphish

Deploy

SMS, Email, WIFI, USB, QR Code, Social Media

Custom tailor the message to fit your campaign

Quickly deploy messages to many users at once
Starphish

Manage

Using a cloud based C2 server

or

A local deployment