Will Android Trojan, Worm or Rootkit Survive in SEAndroid and Containerization?

Rowland Yu & William Lee

Email: {rowland.yu, william.lee}@sophos.com.au

vb 2015 PRAGUE
30 Sept - 2 Oct 2015

Agenda

- Why SEAndroid and Containerization?
- What are SEAndroid and Containerization?
- Doom to fail
- We prove
- The future
- Conclusion

SOPHOS

Why SEAndroid and Containerization?

SEAndroid and Containerization

Access Control

Goals of SEAndroid and Containerization

p://source.android.com/devices/tech/security/selir | Security-Enhanced Linux in...

Favorites Tools Help

Contributions to it have been made by a number of companies and organizations; all Android code and contributors are publicly available for review on android.googlesource.com. With SELinux, Android can better protect and confine system services, control access to application data and system logs, reduce the effects of malicious software, and protect users from potential flaws in code on mobile devices.

http://blogs.csc.com/2015/04/06/google-slashes-andı | Google Slashes Android M...

View Favorites Tools Help

Since that report, it seems Google went to work to improve the security of its Android software.

Through implementing a series of security enhancements, Google says it has managed to reduce the amount of Android malware by half. And according to Google, devices had harmful apps installed, and of those users who install move), that figure came down to 0.15 percent.

According to Google, there were a number of security improvemer encryption, more hardware- protected encryption, and enhanceme sandbox with SELinux-based Mandatory Access Control (MAC). G were provided better tools to find and fix or respond to security vul

http://www.zdnet.com/article/good-technology-partı | Good Technolog

View Favorites Tools Help

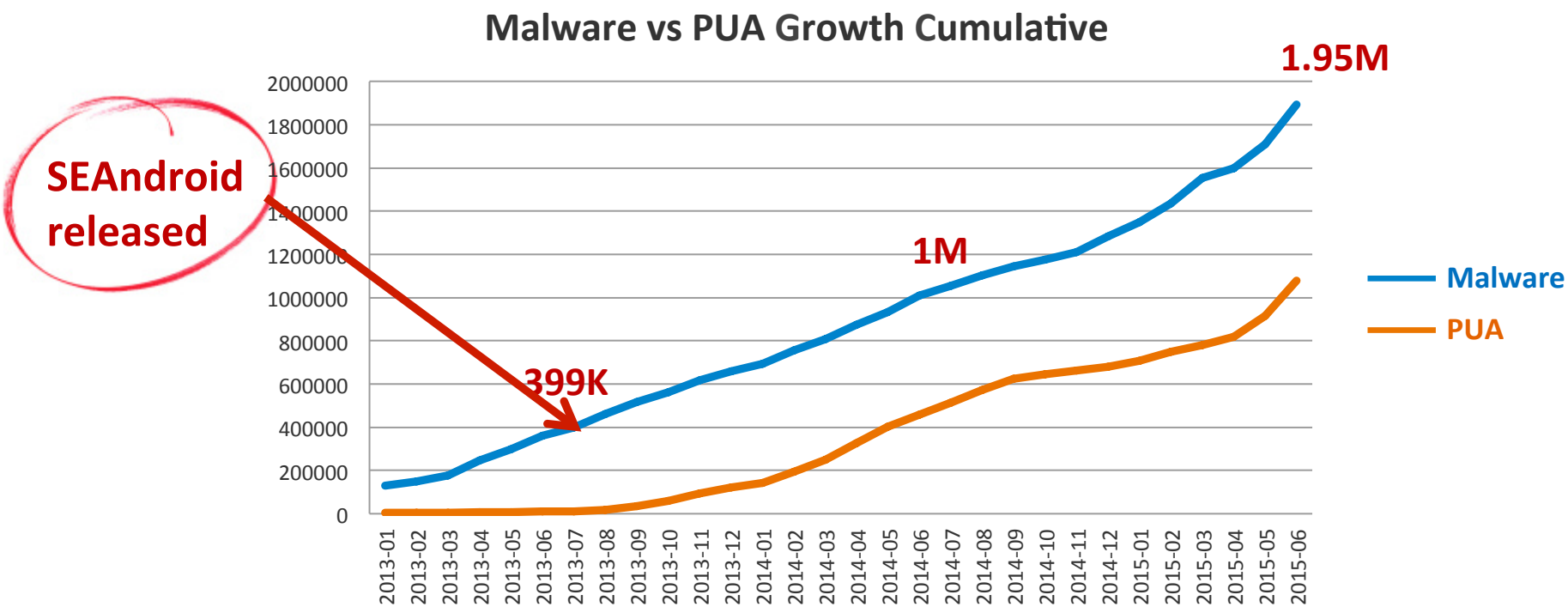
The joint product pairs Good's app container and ecosys with the KNOX enterprise security platform for Android. nutshell, the product works by creating a Good-secured domain within a Knox-secured Android operating systen

According to the two companies, Good for Samsung Kn eliminate virus and malware concerns that come with Ar adoption in the enterprise.

Malware Trend VS Security Enhancements

Version	Codename	API	Distribution	Release Date
4.3	Jelly Bean	18	4.7%	Jul 2013
4.4	KitKat	19	39.3%	Sep 2013
5.0	Lollipop	21	15.5%	Nov 2014
5.1		22	2.6%	

62%



SOPHOS

What is SEAndroid?

Android Security Model

- DAC (Discretionary Access Control)
  - Each App has its own UID/GID for app isolation.
  - The file owner makes decision for the file access.
  - Owner(rwx):Group(rwx):Others(rwx)
    - drwxr-x--x system system com.android.settings
    - drwxr-x--x u0_a15 u0_a15 com.android.browser
- App Permissions
  - Each App has requested Permissions such as SEND_SMS/INTERNET.
  - Granted Permissions are allowed.

DAC Weaknesses

- No system-wide security policy as Access control is based on the discretion of the file owner.
- Flawed or malicious applications can bypass permission system and escalate their privileges.
- Inability to confine any system daemons or setuid programs that run with the root.

Mandatory Access Control (MAC)

```
ps -Z
u:r:system_app:s0    system com.android.settings
u:r:untrusted_app:s0 u0_a15 com.android.browser
```

Subject

Process #0

Domain

Access?

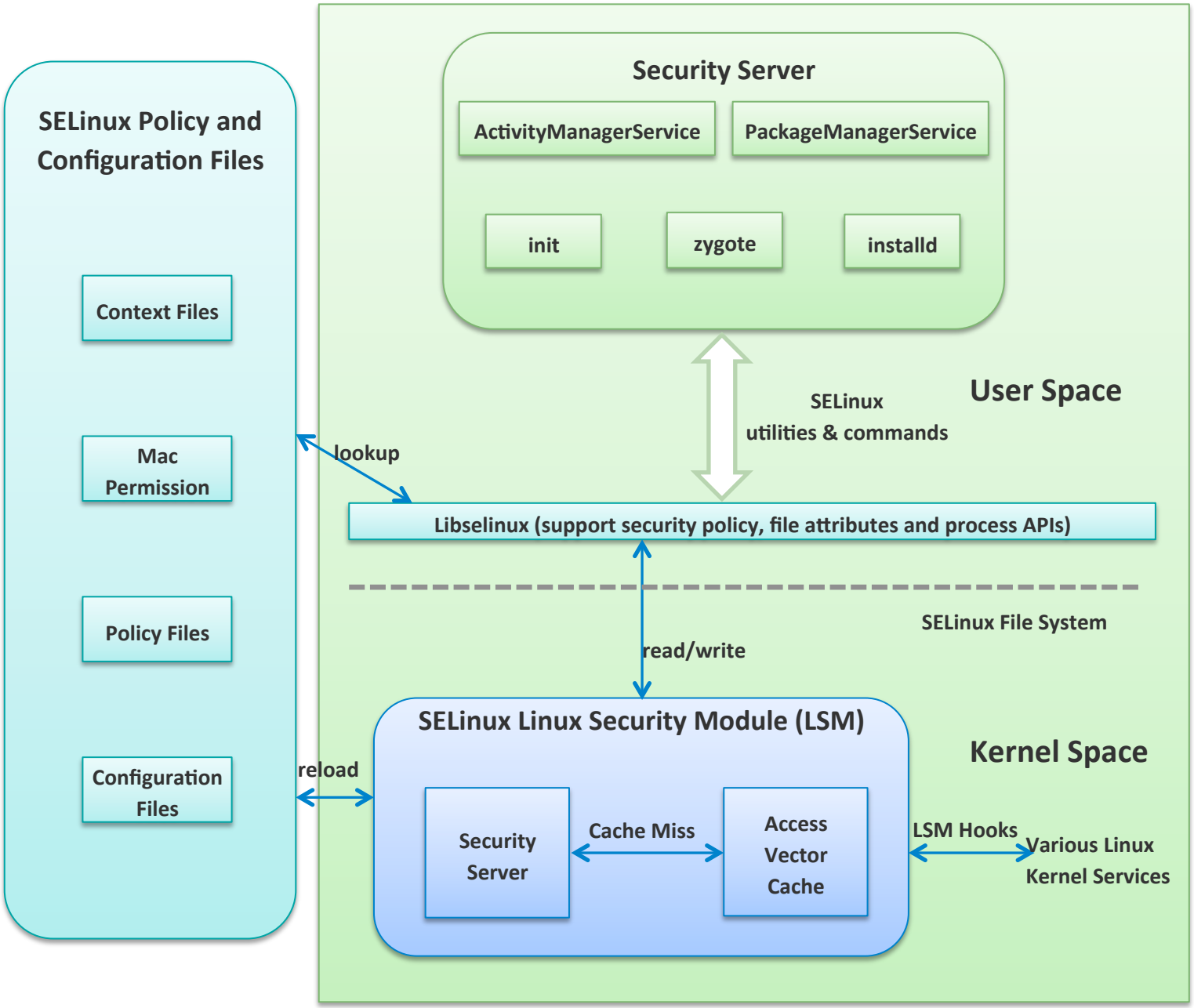
Rules Database

Objects

Class

```
<av_action> <subject...> <object...>:<class...> { <permissions...> }
allow appdomain system_data_file:dir r_dir_perms;
```

The overview of SEAndroid Framework



mac_permissions.xml – Middleware MAC (MMAC)

The file is used for the **install-time check** of application permissions against the MAC policy. It utilizes the **value of signature and *seinfo* tags** to assign policy stanzas for a given app or all apps from either platform or third-parties.

```
<?xml version="1.0" encoding="utf-8"?>
<policy>
<!-- Sample signer stanza for install policy
Rules:  Sample stanzas are given below based on the AOSP developer keys.
-->
    <!-- Platform dev key with AOSP -->
    <signer signature="....b357" >
      <allow-all />
      <seinfo value="platform" />
    </signer>
    <!-- shared dev key in AOSP -->
    <signer signature="...6f84" >
      <allow-permission name="android.permission.ACCESS_COARSE_LOCATION" />
      <allow-permission name="android.permission.CALL_PHONE" />
      ....
      <seinfo value="shared" />
    </signer>
    <!-- All other keys -->
    <default>
      <seinfo value="default" />
      <deny-permission name="android.permission.ACCESS_COARSE_LOCATION" />
      <deny-permission name="android.permission.CALL_PHONE" />
      ....
    </default>
</policy>
```

mac_permissions.xml from a Nexus 5 running on Android 5.1

```
<?xml version="1.0" encoding="iso-8859-1"?>
<!-- AUTOGENERATED FILE DO NOT MODIFY -->
<policy>
<signer signature="...e26a">
    <seinfo value="platform"/>
</signer>
<default>
    <seinfo value="default"/>
</default>
</policy>
```

SEAndroid with Root Exploits

- GingerBreak
  - Following MAC policy rejected execution of a binary from the data partition from vold.
  - **neverallow** appdomain system_file:dir_file_class_set { create write setattr relabelfrom relabelto append unlink link rename }
- RageAgaintTheCage
  - Following MAC policy rejected transitions to the privileged security context and remounting system partition.
  - **neverallow** { appdomain -shell userdebug_or_eng(`-su') } { domain -appdomain }:process { transition dyntransition };

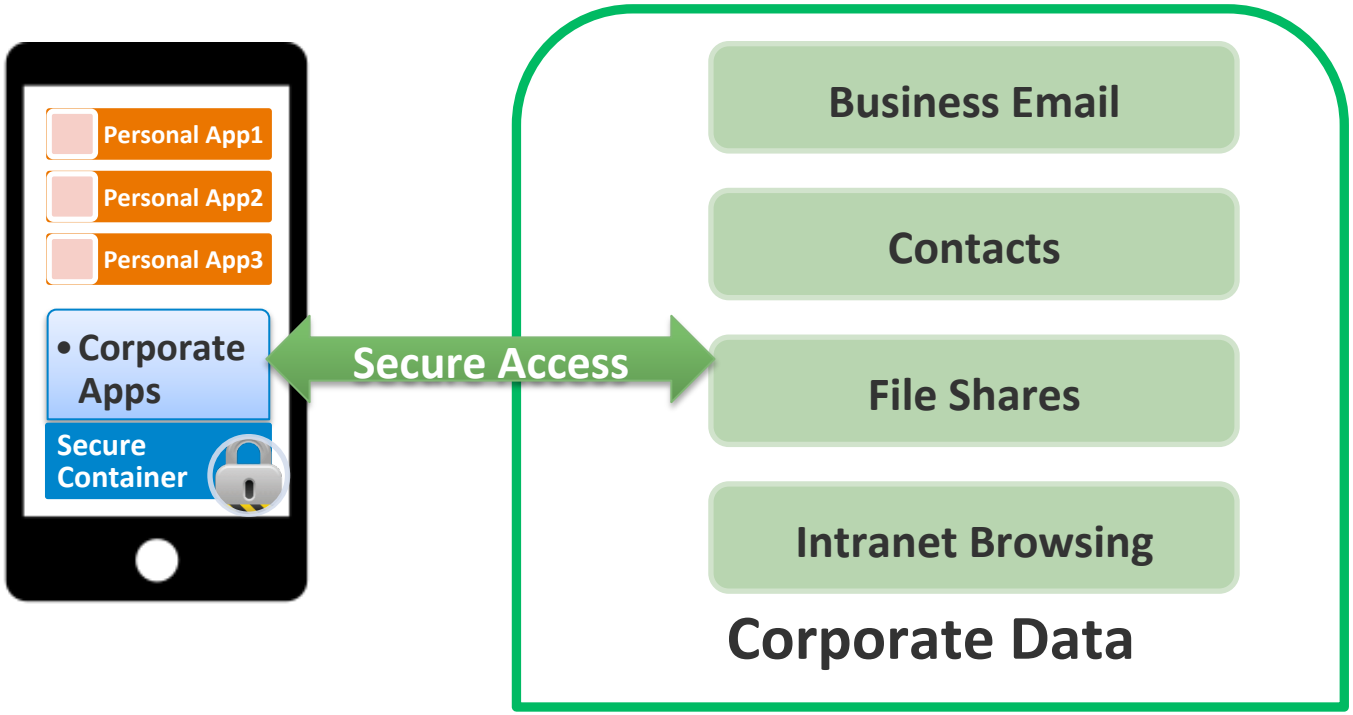
SOPHOS

What is Containerization?

Containerization (Secure Container)

- Design for BYOD (bring your own device)
- Be Adopted in mobile device management (MDM)
- Securely access to corporate data
- Prevent the misuse of malware, intruders or other apps

Containerization (Secure Container)



SOPHOS

Doom to Fail

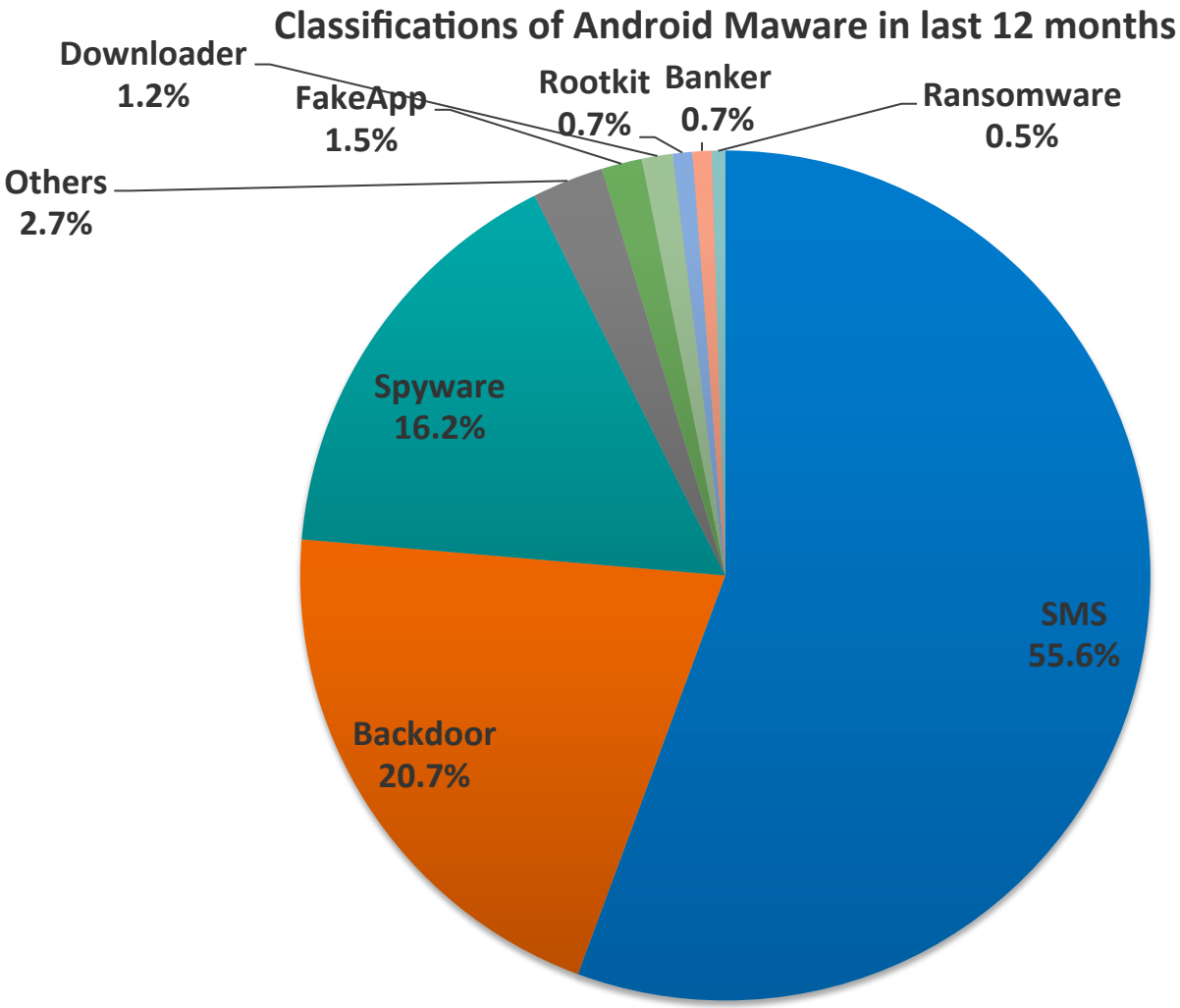
Why?

- Permissions are the key to control access
- Social Engineering
- Vulnerabilities and exploits subvert Android system
- Compatibility problems then break other functionalities
- Android Fragmentation
- …….

SOPHOS

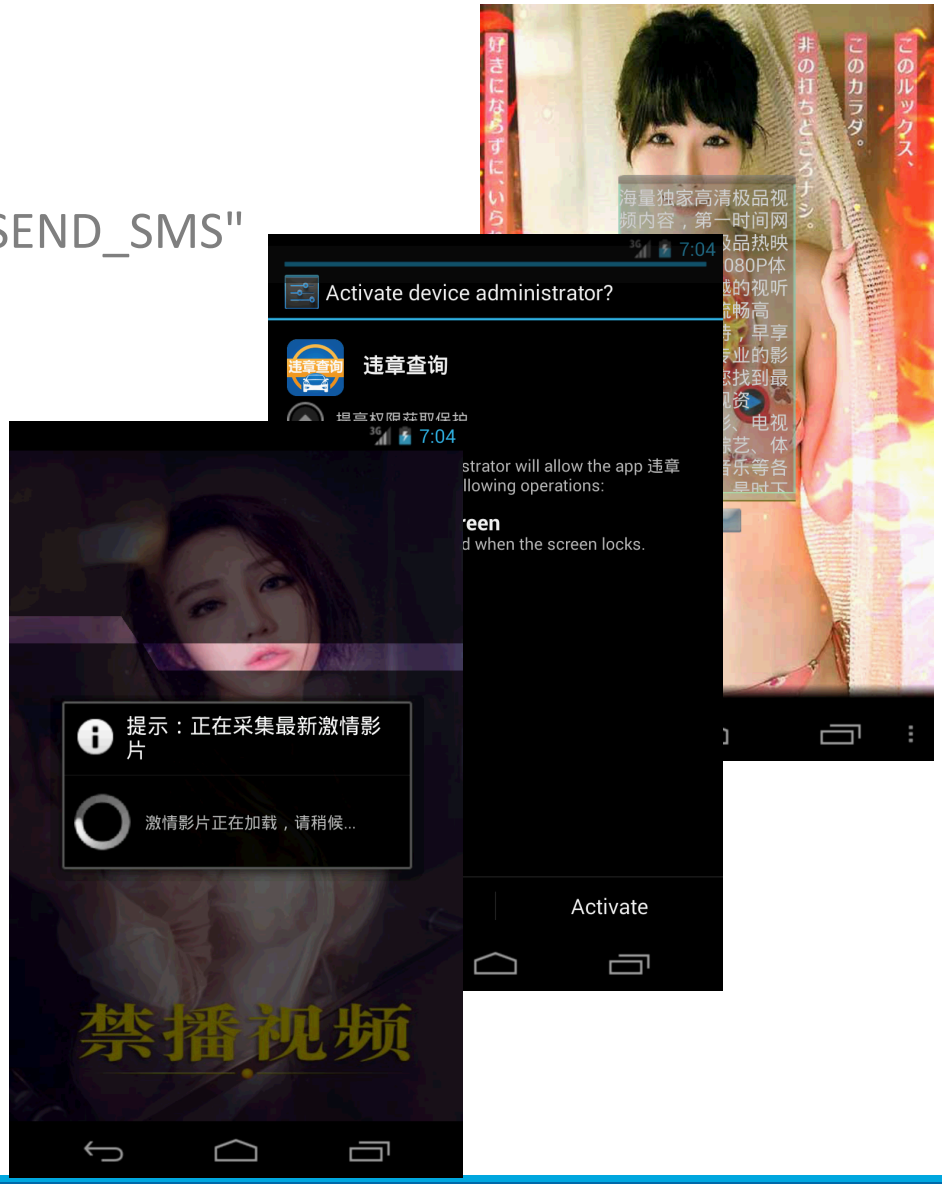
We Prove

The survival of existing Android malware



Premium SMS Sender

- Easiness
  - Permission: "android.permission.SEND_SMS"
  - *sendTextMessage* () method
- Social engineering
- Demo…



Backdoor

- Set up or distribute via mobile Botnet
- Send or intercept SMS messages
- Download, install, or activate any Android app without user knowledge
- Make arbitrary phone call
- Clear user data, uninstall existing applications, or disable system applications
- Upload sensitive information including device id, locations, application usage, call log and SMS history to remote websites
- Execute command & control services
- Quick Demo ……

Backdoor Cont.

CoolReaper hidden in a legitimate ROM image

Coolpad Dazen F2 8675-W00 - Specifications

Width | Height | Thickness | Weight | Write a review

Specifications | Display | Camera | CPU | Battery

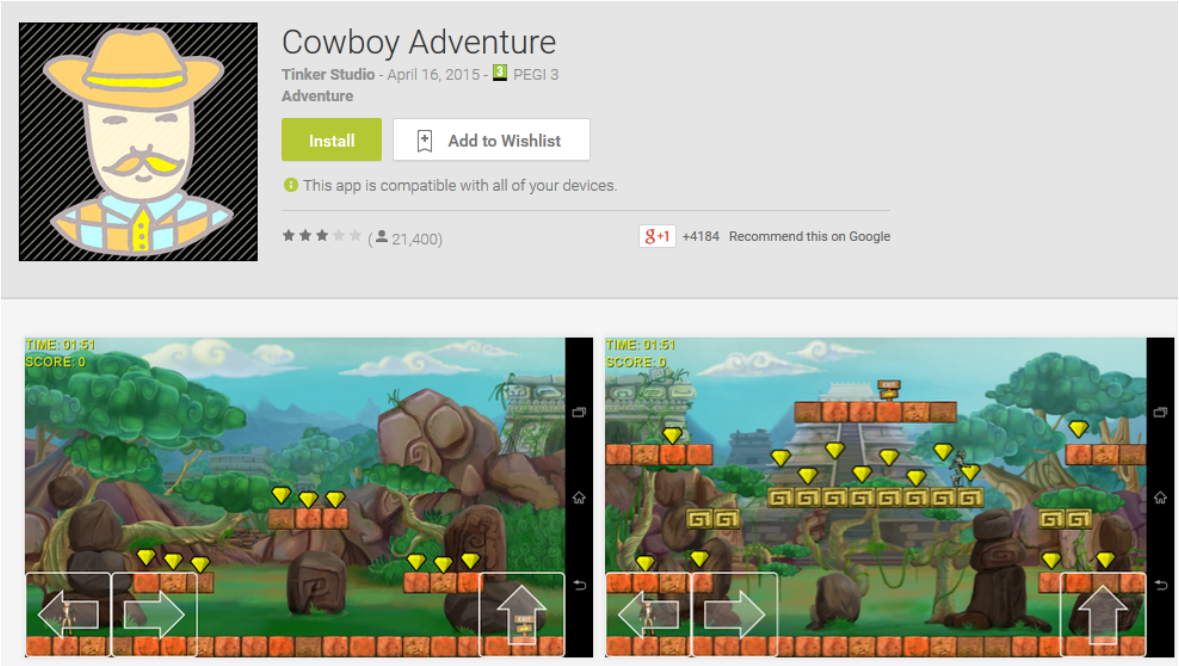
Dimensions: 78 x 154.5 x 8.6 mm
Weight: 154 g
SoC: Qualcomm Snapdragon 615 MSM8939
CPU: 4x 1.5 GHz ARM Cortex-A53, 4x 1.0 GHz
GPU: Qualcomm Adreno 405, 550 MHz
RAM: 2 GB, 800 MHz
Storage: 16 GB
Memory cards: microSD, microSDHC, microSD
Display: 5.5 in, IPS, 720 x 1280 pixels, 24 bit
Battery: 2500 mAh, Li-Polymer
OS: Android 4.4.2 KitKat
Camera: 4128 x 3096 pixels, 1920 x 1080 pixe
SIM card: Micro-SIM
Wi-Fi: b, g, n
USB: 2.0, Micro USB
Bluetooth: 4.0
Positioning: GPS, A-GPS

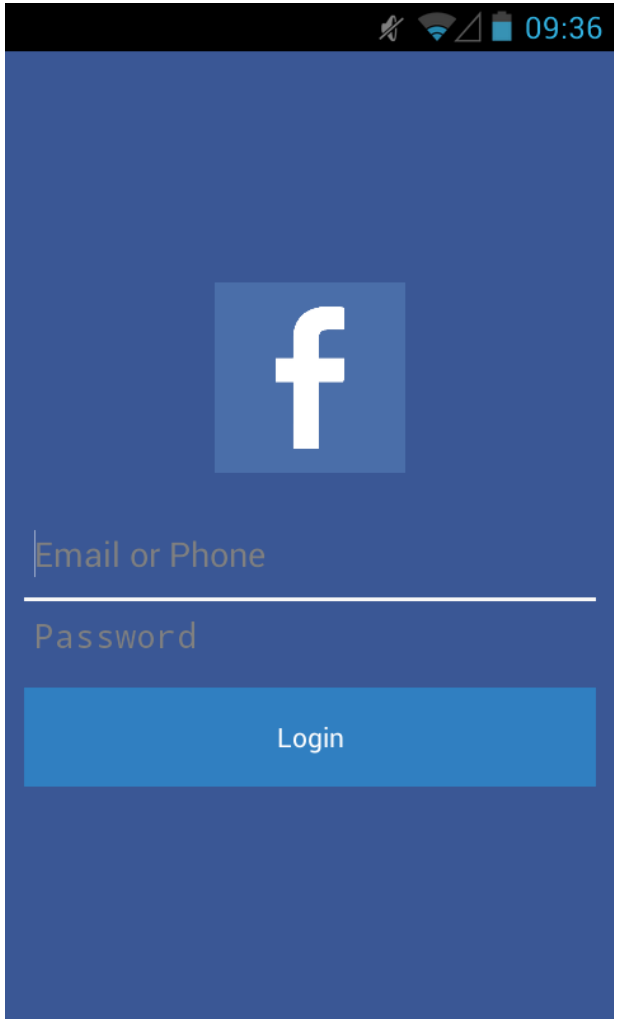
Add for comparison | Suggest

Spyware & Banker Trojan

Social Engineering

Spyware & Banker Trojan cont.





Permissions:

- INTERNET
- ACCESS_NETWORK_STATE
- WRITE_EXTERNAL_STORAGE

FakeAV and Ransomware

- Fake alerts to scare victims to pay money
- Permissions:

uses-permission:'android.permission.WAKE_LOCK’

Or

uses-permission:'android.permission.SYSTEM_ALERT_WINDOW’

uses-permission:'android.permission.READ_EXTERNAL_STORAGE'

uses-permission:'android.permission.WRITE_EXTERNAL_STORAGE

FakeAV and Ransomware

```
v0.scheduleAtFixedRate(new Runnable() {
    public void run() {
        if(!MainService.this.settings.getBoolean("DISABLE_LOCKER", false) && !Main.isRunning) {
            Intent v0 = new Intent(MainService.this, Main.class);
            v0.addFlags(268435456);
            v0.addFlags(131072);
            MainService.this.startActivity(v0);
        }
    }
}, 1, 1, TimeUnit.SECONDS);
```

```
private void createFloatView() {
    this.btn_floatView = new Button(this.getApplicationContext());
    this.btn_floatView.setText("");
    FloatingWindowService.wm = this.getApplicationContext().getSystemServi
    FloatingWindowService.params = new WindowManager$LayoutParams();
    FloatingWindowService.params.type = 2010;
    FloatingWindowService.params.format = 1;
    FloatingWindowService.params.flags = 40;
    this.btn_floatView.setBackgroundResource(2130837505);
    FloatingWindowService.params.width = 300;
    FloatingWindowService.params.height = 50;
    FloatingWindowService.params.gravity = 51;
    FloatingWindowService.params.x = 0;
    FloatingWindowService.params.y = 0;
    this.btn_floatView.setOnTouchListener(new 100000002(this));
    FloatingWindowService.wm.addView(this.btn_floatView, FloatingWindowSe
    this.isAdded = true;
}
```

FakeAV and Ransomware

- Demo…

Vulnerabilities

- Samsung Pre-installed Swift Keyboard Security Risk : Over 600M+ Devices Worldwide Impacted
- CVE-2015-4640 and CVE-2015-4641
  - Language files are downloaded via HTTP
  - Keyboard was signed with Samsung's private key

```
aapt d xmltree SamsungIME.apk AndroidManifest.xml | grep shared
        A: android:sharedUserId(0x0101000b)="android.uid.system" (Raw:
"android.uid.system")
```

Vulnerabilities cont.

- Stagefright – C++ software library for playing multimedia files
- Attack vector exploits contain integer overflow vulnerabilities

Mitigation Summary of StageFright

Mitigation	Applicability
SELinux/SEAndroid	N/A
Stack Cookies	N/A
FORTIFY_SOURCE	N/A
ASLR	Only Android >= 4.0
NX	Bpass with ROP
GCC new[] mitigation	N/A*

ASLR (Address space layout randomization) is the ONLY challenge.

^ From Joshua "jduck" Drake August 5th 2015 Black Hat USA

Rootkit & Bootkit

- Customized ROM
- Oldboot …

SOPHOS

The Future

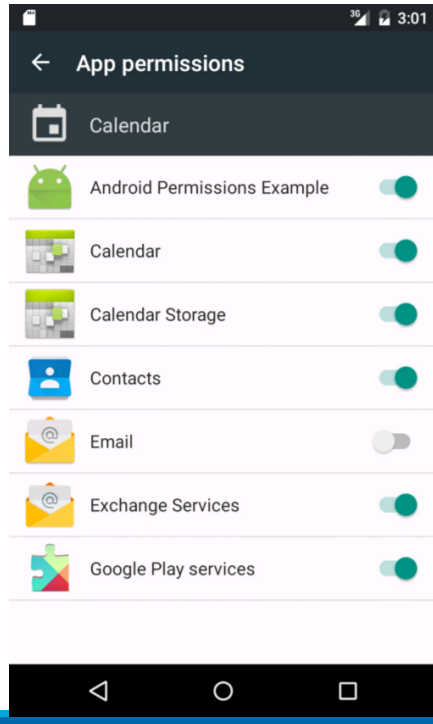
- Android permission model is the key to control (Android M)
- Uprising trends will keep dominating Android malware attacks
- Getting smarter and aiming to generate more profit
  - SMS Sender – (game, fakeapp, porn …)
  - Social Engineering
  - Diversified and Multichannel
  - Taking advantage of Android Fragmentation
  - …

SOPHOS

Conclusion

Conclusion

- Everything is in enforcement since the 5.0 release
- By 2017, 65 percent of enterprises will adopt MDM
- Volume and sophisticated
- Android M 6.0 introduces a new permissions model
- More attack vectors than before
- Vehicle and wearable based malware



SOPHOS

Q&A