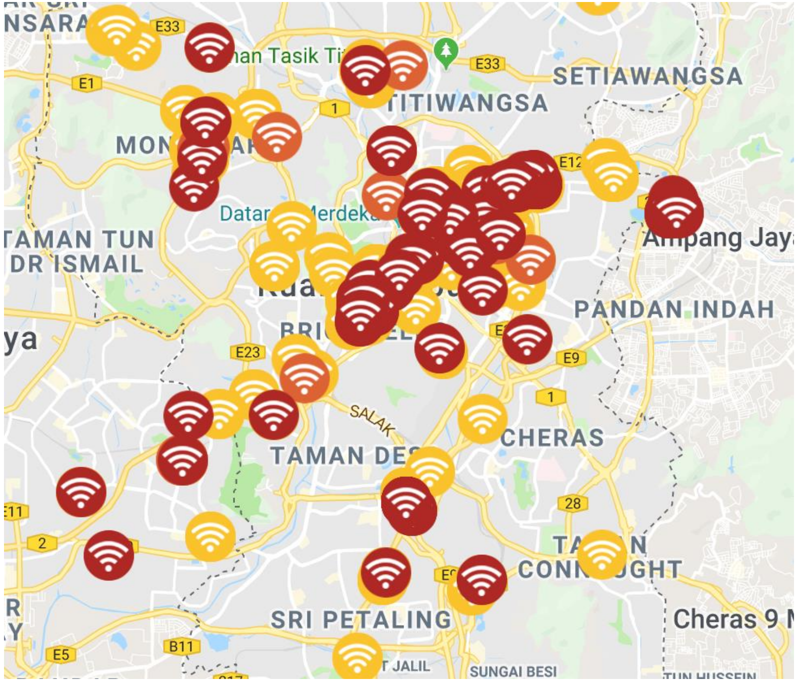
Mobile Defence in a time of Uncertainty

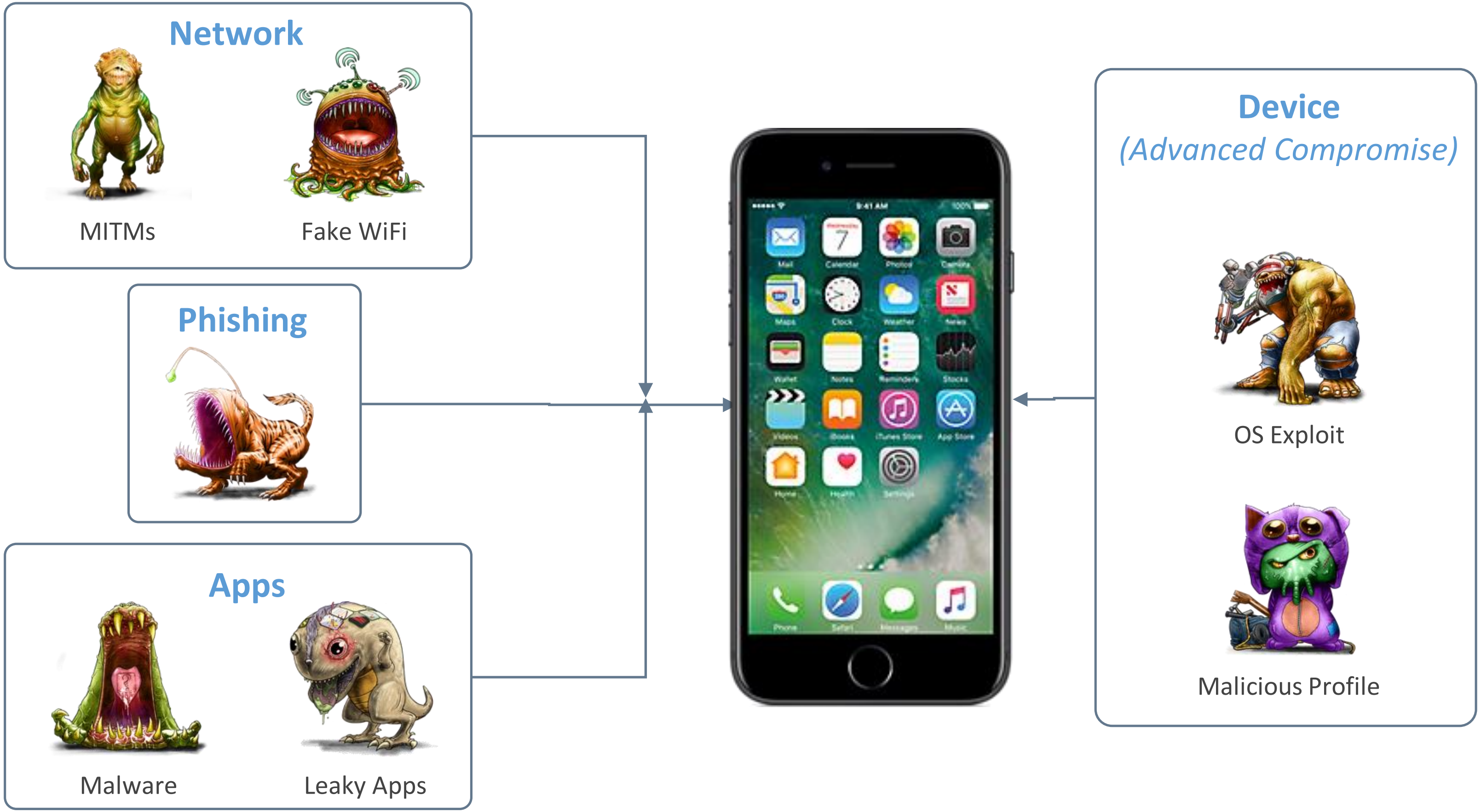
Pat Shueh - VP Solution Engineering - Asia Pacific & Japan

How secure is your mobile?



- **Are you running the latest version?**
  - Security Updates / Fixes (30+ updates)
- **Mobile Malware is 30%** of all Malware, increase of Fake Apps and **Leaky Apps**
- **1 in 5** device experience network attack
- Phishing attack over **Social Media/SMS**
- Devices are compromised from loading **photo, surfing website, iMessage, YouTube, USB charger, Bluetooth, WhatsApp …etc**

Common Mobile Attack Vectors



Network

MITMs

Fake WiFi

Phishing

Apps

Malware

Leaky Apps

Device

(Advanced Compromise)

OS Exploit

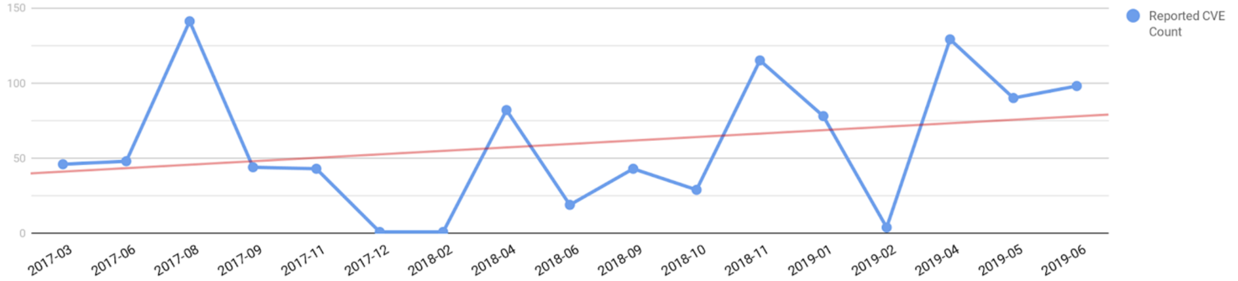
Malicious Profile

Take Control, Stay Hidden

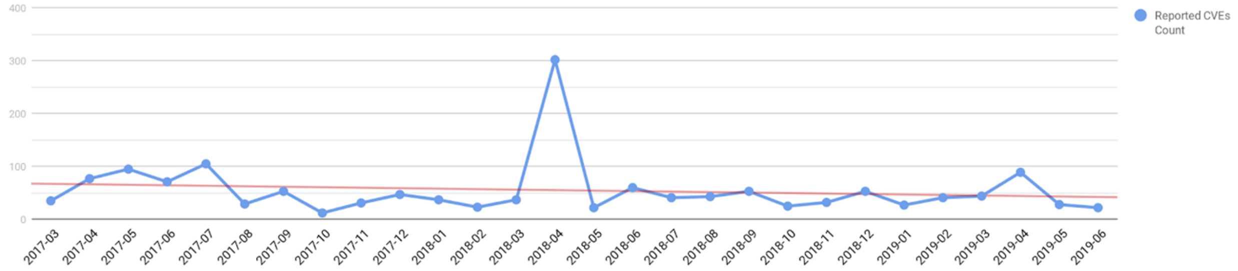
Which OS is More Secure?

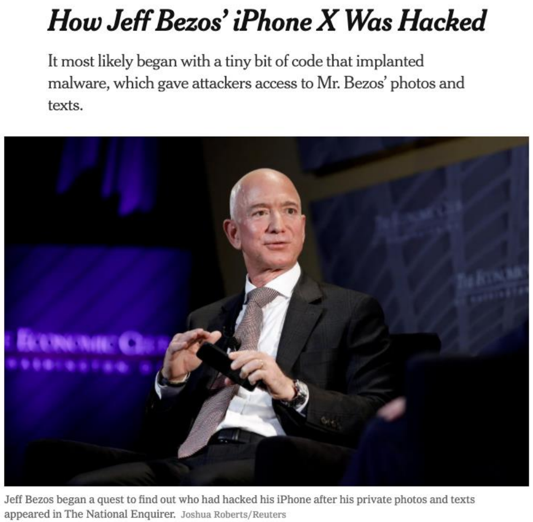
OS Risk Trend over time

Critical and Medium CVEs per Month for iOS



Critical and High Severity CVEs per Month for Android





How Jeff Bezos' iPhone X Was Hacked

It most likely began with a tiny bit of code that implanted malware, which gave attackers access to Mr. Bezos' photos and texts.

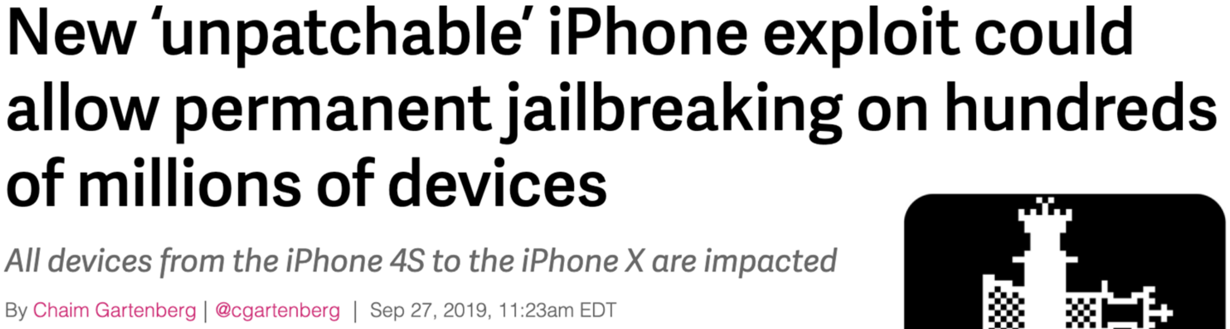
Jeff Bezos began a quest to find out who had hacked his iPhone after his private photos and texts appeared in The National Enquirer. Joshua Roberts/Reuters

How?

4.4MB video received over WhatsApp implemented spyware

So What?

Attacker use the hardware bug in iPhone to compromise the device.

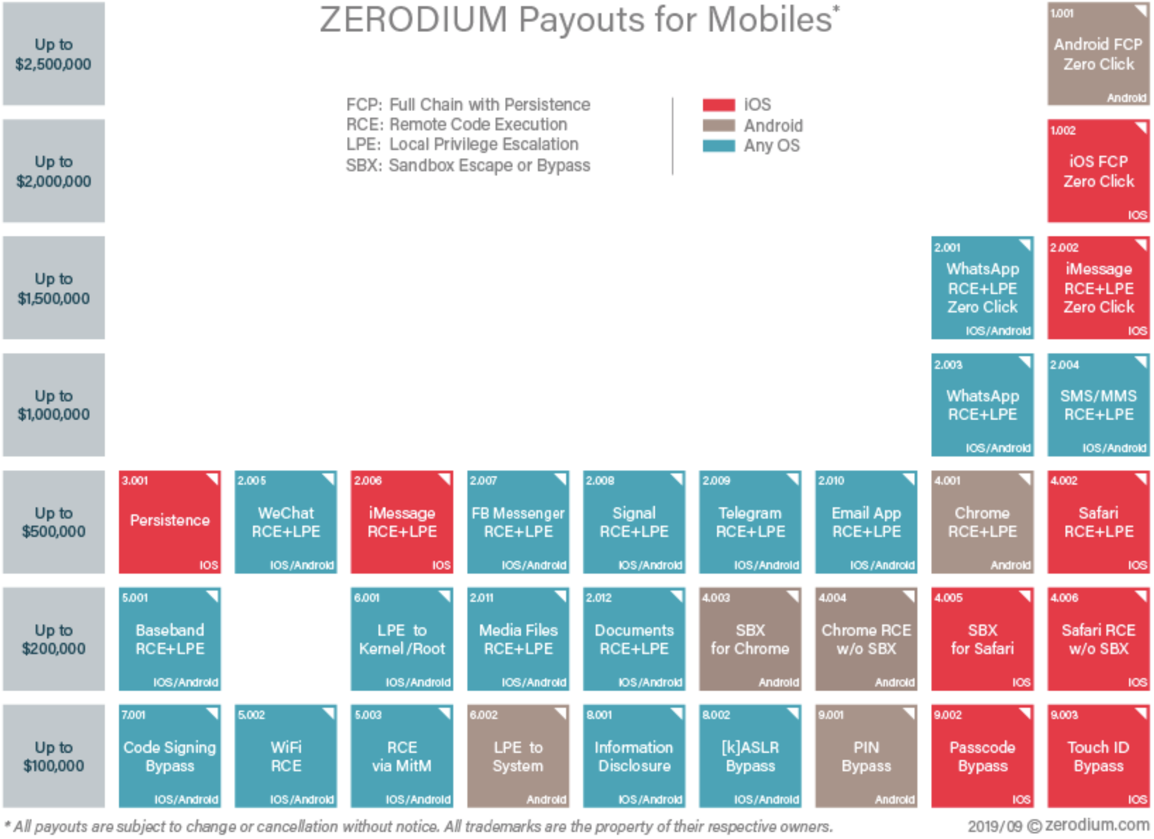


New 'unpatchable' iPhone exploit could allow permanent jailbreaking on hundreds of millions of devices

All devices from the iPhone 4S to the iPhone X are impacted

By Chaim Gartenberg | @cgartenberg | Sep 27, 2019, 11:23am EDT

I’m running the latest version - So I am safe?



ZERODIUM Payouts for Mobiles*

FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

🟥 iOS
🟫 Android
🟦 Any OS

Up to $2,500,000									1.001 Android FCP Zero Click Android
Up to $2,000,000									1.002 iOS FCP Zero Click iOS
Up to $1,500,000								2.001 WhatsApp RCE+LPE Zero Click iOS/Android	2.002 iMessage RCE+LPE Zero Click iOS
Up to $1,000,000								2.003 WhatsApp RCE+LPE iOS/Android	2.004 SMS/MMS RCE+LPE iOS/Android
Up to $500,000	3.001 Persistence iOS	2.005 WeChat RCE+LPE iOS/Android	2.006 iMessage RCE+LPE iOS	2.007 FB Messenger RCE+LPE iOS/Android	2.008 Signal RCE+LPE iOS/Android	2.009 Telegram RCE+LPE iOS/Android	2.010 Email App RCE+LPE iOS/Android	4.001 Chrome RCE+LPE Android	4.002 Safari RCE+LPE iOS
Up to $200,000	5.001 Baseband RCE+LPE iOS/Android		6.001 LPE to Kernel/Root iOS/Android	2.011 Media Files RCE+LPE iOS/Android	2.012 Documents RCE+LPE iOS/Android	4.003 SBX for Chrome Android	4.004 Chrome RCE w/o SBX Android	4.005 SBX for Safari iOS	4.006 Safari RCE w/o SBX iOS
Up to $100,000	7.001 Code Signing Bypass iOS/Android	5.002 WiFi RCE iOS/Android	5.003 RCE via MitM iOS/Android	6.002 LPE to System Android	8.001 Information Disclosure iOS/Android	8.002 [k]ASLR Bypass iOS/Android	9.001 PIN Bypass Android	9.002 Passcode Bypass iOS	9.003 Touch ID Bypass iOS

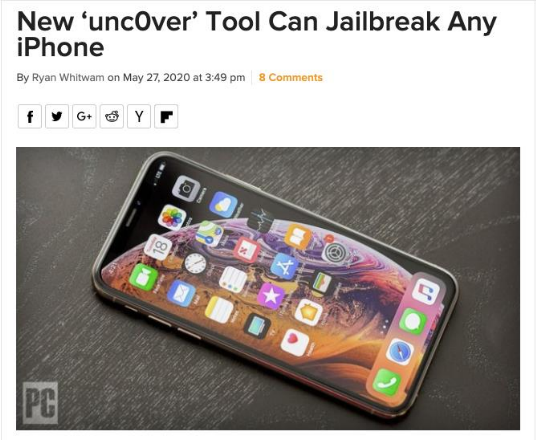
* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/09 © zerodium.com

2020

Zero Day

<u>$2.5M vs $2M</u> Full Control

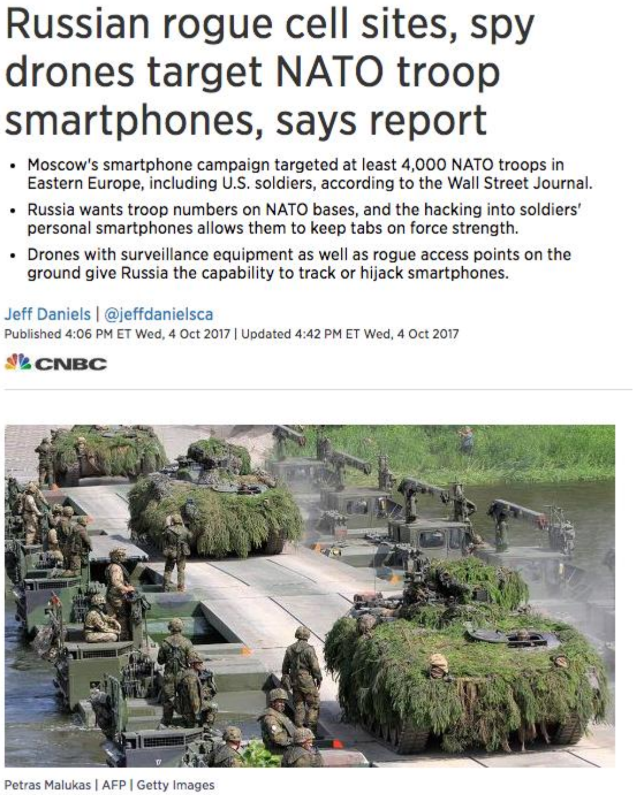


New ‘unc0ver’ Tool Can Jailbreak Any iPhone

By Ryan Whitwam on May 27, 2020 at 3:49 pm | 8 Comments

<u>13.5</u>

WiFi network are vulnerable



Russian rogue cell sites, spy drones target NATO troop smartphones, says report

- Moscow's smartphone campaign targeted at least 4,000 NATO troops in Eastern Europe, including U.S. soldiers, according to the Wall Street Journal.
- Russia wants troop numbers on NATO bases, and the hacking into soldiers' personal smartphones allows them to keep tabs on force strength.
- Drones with surveillance equipment as well as rogue access points on the ground give Russia the capability to track or hijack smartphones.

Jeff Daniels | @jeffdanielsca

Published 4:06 PM ET Wed, 4 Oct 2017 | Updated 4:42 PM ET Wed, 4 Oct 2017

CNBC

Petras Malukas | AFP | Getty Images

Personal
Email

I am coming at you!

SMS &
Messaging Apps

Phishing

90% Of Breaches Start With A Phishing Attack[1]

61% Of Emails Are Opened On Mobile Devices[2]

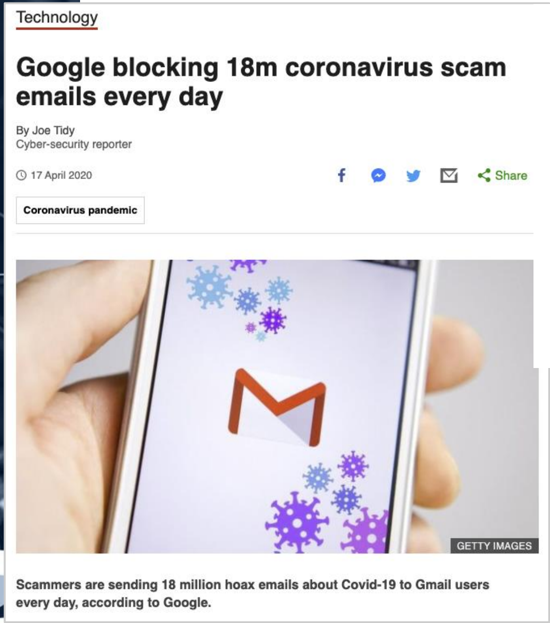
[1] Verizon Data Breach Investigations Report, 2018
[2] Adestra, 2018

Phishing targets mobile

- 2FA password
- Credential theft
- Advanced Attack

Average lifespan of phishing site

10 days



Technology

Google blocking 18m coronavirus scam emails every day

By Joe Tidy
Cyber-security reporter

17 April 2020

Share

Coronavirus pandemic

GETTY IMAGES

Scammers are sending 18 million hoax emails about Covid-19 to Gmail users every day, according to Google.

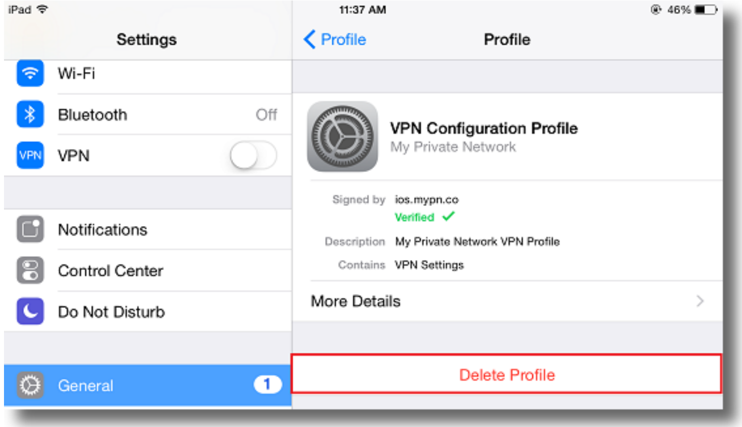
PayPal (37.44%)
Facebook (10.62%)
Microsoft (8.73%)
Steam (6.02%)
ABSA Bank (3.44%)
Blockchain (3.35%)
eBay (2.87%)
RuneScape (2.86%)
Amazon.com (2.15%)
Apple (1.77%)

Phishing Brands vs Phishing Domains

US (58.74%)
CN (12.18%)
DE (5.75%)
CA (5.61%)
JP (2.93%)
IN (2.54%)
FR (1.94%)
GB (1.44%)
ES (0.71%)
NL (0.66%)
TR (0.64%)
MY (0.63%)
DK (0.61%)
KY (0.60%)
HK (0.57%)
RU (0.56%)
KR (0.55%)
AU (0.54%)
Other (2.24%)

I am the malware for iOS!

iOS Profiles



iPad 11:37 AM 46%

Settings

- Wi-Fi
- Bluetooth Off
- VPN
- Notifications
- Control Center
- Do Not Disturb
- General 1

< Profile Profile

VPN Configuration Profile
My Private Network

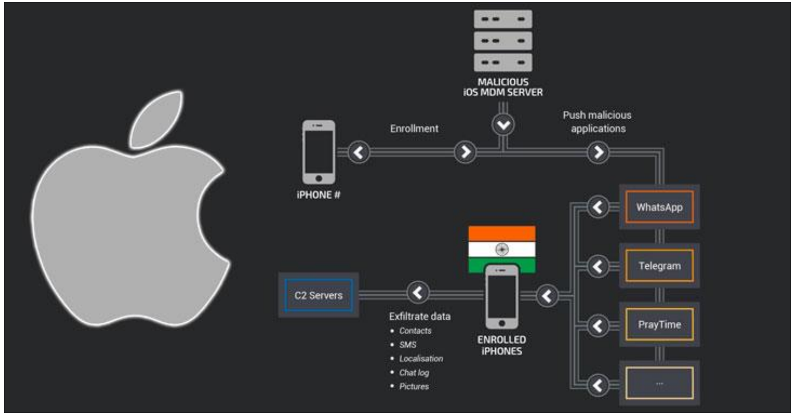
Signed by	ios.mypn.co Verified ✓
Description	My Private Network VPN Profile
Contains	VPN Settings

More Details >

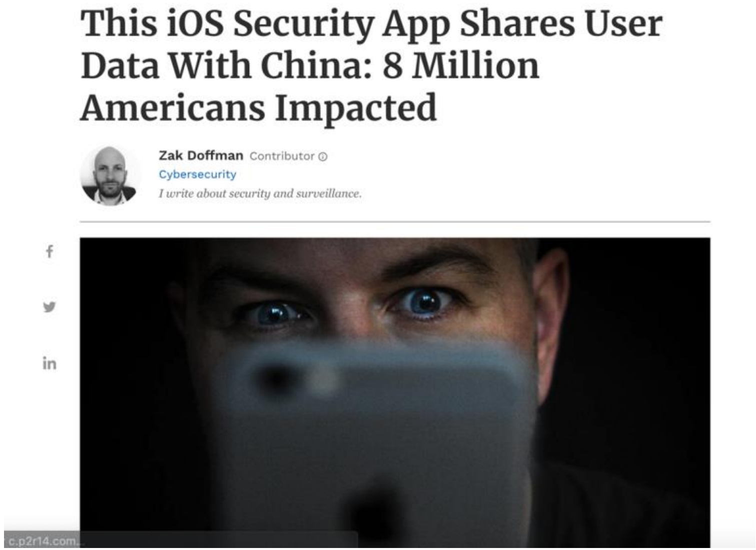
Delete Profile

iOS Profiles more prevalent than malware on iOS

- ‘sideload’ appstores
- wifi / proxy configurations
- Personal VPN profiles
- ”Jailbreak” profiles (CA / store / exploit)
- Unmanaged Root CA certificates



Hacked MDM Server to push down malware



This iOS Security App Shares User Data With China: 8 Million Americans Impacted

Zak Doffman Contributor
Cybersecurity
I write about security and surveillance.

c.p2r14.com...

User data shared via profile

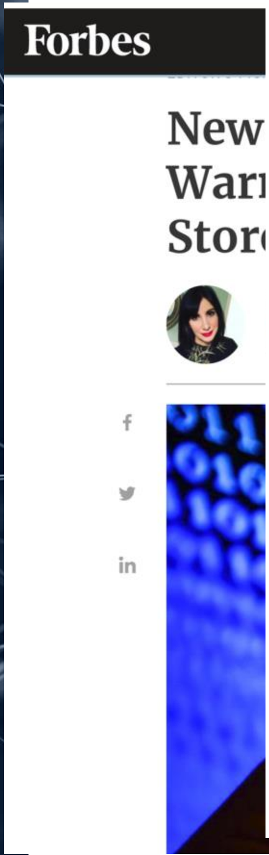
Born to be Bad

Can be bad

Malware & Leaky App

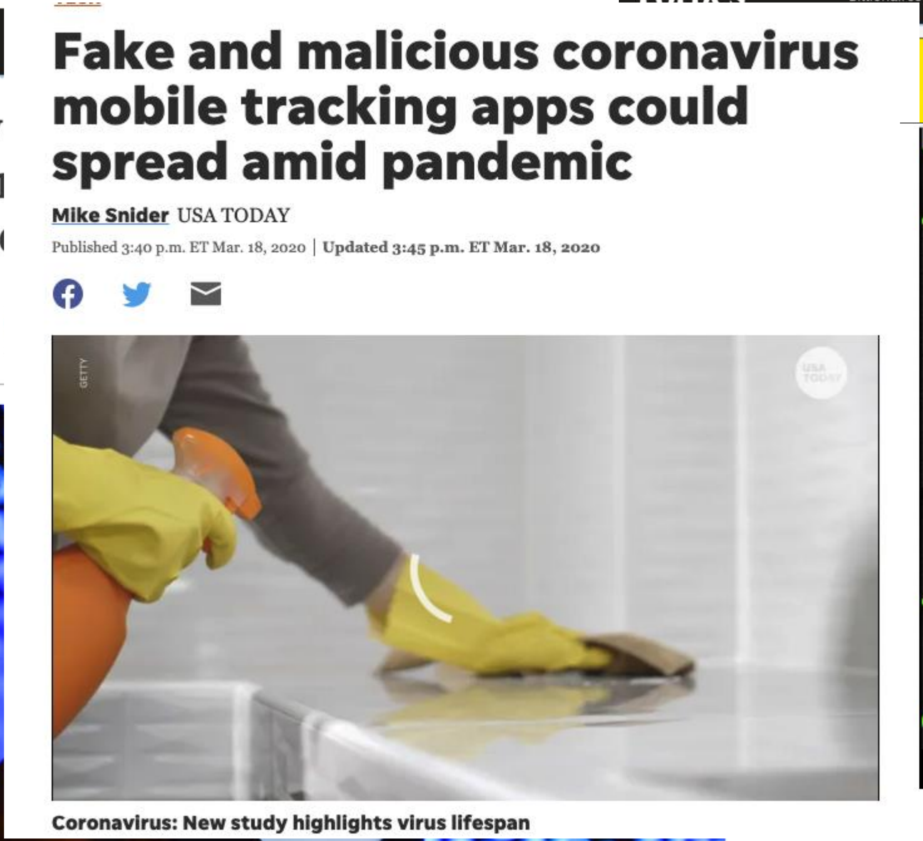
- *How many apps on your device have access to your clipboard, photos, location, microphone, camera, messages?*

Malware, Trojan, Ransomware



Forbes

New
Warr
Stor

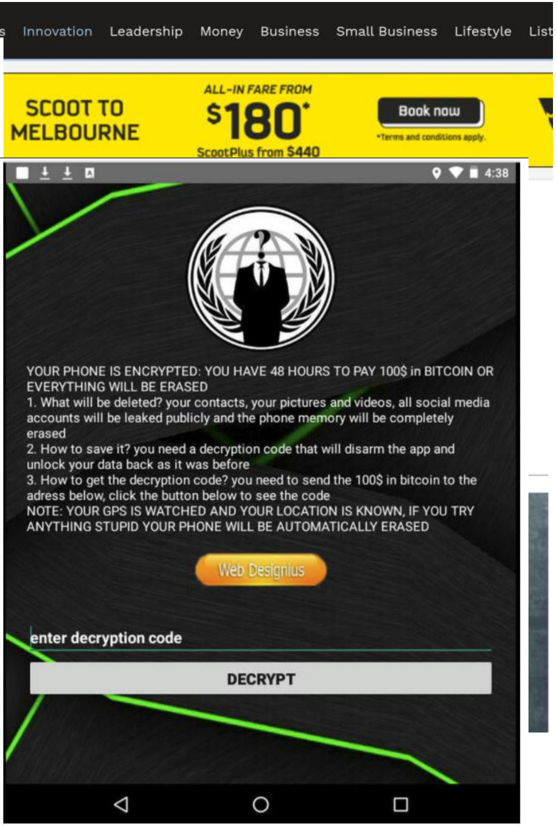


Fake and malicious coronavirus mobile tracking apps could spread amid pandemic

Mike Snider USA TODAY

Published 3:40 p.m. ET Mar. 18, 2020 | **Updated 3:45 p.m. ET Mar. 18, 2020**

Coronavirus: New study highlights virus lifespan



Forbes

YOUR PHONE IS ENCRYPTED: YOU HAVE 48 HOURS TO PAY 100$ in BITCOIN OR EVERYTHING WILL BE ERASED

1. What will be deleted? your contacts, your pictures and videos, all social media accounts will be leaked publicly and the phone memory will be completely erased

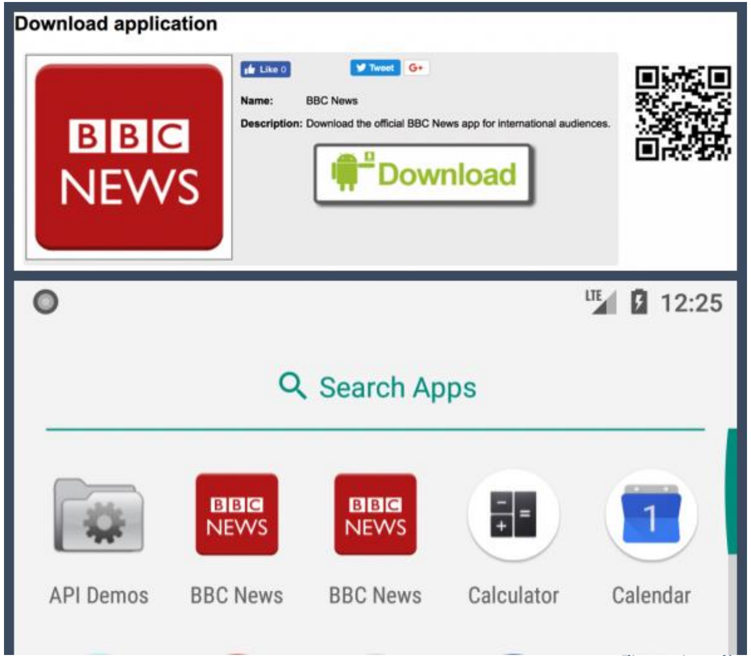
2. How to save it? you need a decryption code that will disarm the app and unlock your data back as it was before

3. How to get the decryption code? you need to send the 100$ in bitcoin to the adress below, click the button below to see the code

NOTE: YOUR GPS IS WATCHED AND YOUR LOCATION IS KNOWN, IF YOU TRY ANYTHING STUPID YOUR PHONE WILL BE AUTOMATICALLY ERASED

Fake App / Leaky App

Which one is real BBC?

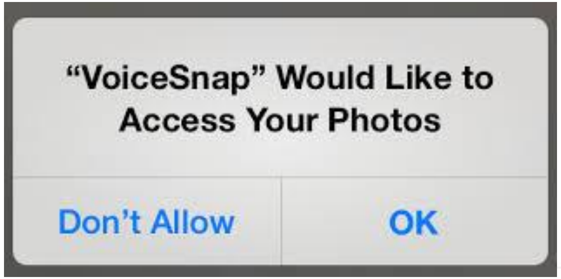


Download application

Name: BBC News

Description: Download the official BBC News app for international audiences.

What permission do you give up?



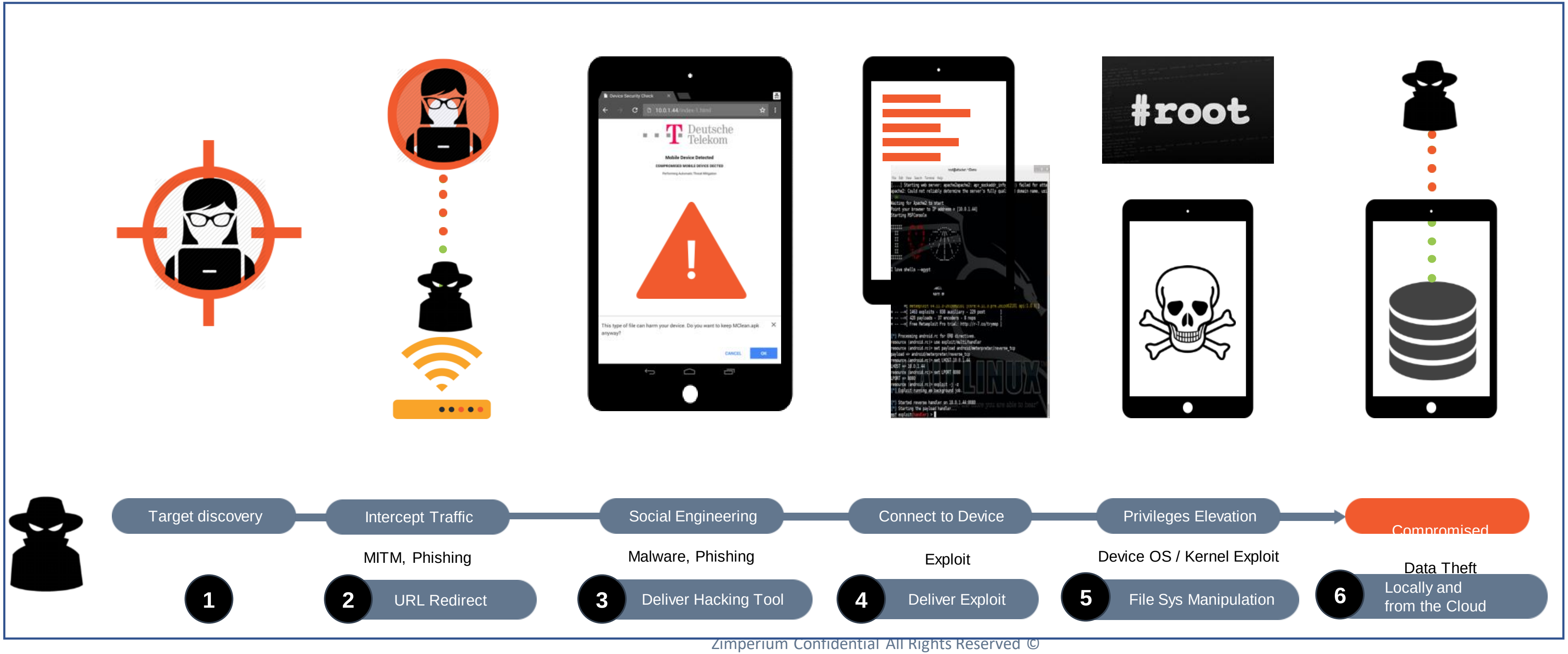
“VoiceSnap” Would Like to Access Your Photos

Demo - iPhone

Disclaimer

How You Were Compromised

The mobile attack Kill Chain



Device Security Check

10.0.1.44/index-1.html

Deutsche Telekom

Mobile Device Detected

COMPROMISED MOBILE DEVICE DECTED

Performing Automatic Threat Mitigation

This type of file can harm your device. Do you want to keep MClean.apk anyway?

CANCEL OK

Target discovery

1

Intercept Traffic

MITM, Phishing

2 URL Redirect

Social Engineering

Malware, Phishing

3 Deliver Hacking Tool

Connect to Device

Exploit

4 Deliver Exploit

Privileges Elevation

Device OS / Kernel Exploit

5 File Sys Manipulation

Compromised

Data Theft

6 Locally and from the Cloud

Mobile Security Tips

- Keep your device up to date
- Ensure downloading apps only from official stores

Trust but Verify - Don't Click “YES” too quickly

- Pay attention to
  - permission you give to the App
  - links you receive
- Use VPN app when you are on open/free WiFi
- Install Mobile Security app (active protection)

Thank You

Speak to you in QnA