Not too long ago, but from very far away…
INVESTIGATING REBEL SCUM’S GOOGLE HOME DATA

Phill Moore
INVESTIGATING REBEL SCUM'S GOOGLE HOME DATA

Phill Moore
YOU PASSED.
WELCOME TO THE DARK SIDE
DARTH AND THE CREW
Who am I?

Digital Forensic Analyst (2011+)

- Bsc (Information Systems)
- Mcyber (Digital Forensics)
- CFCE
- GCFE
- GCFA

This Week in 4n6 (2016+)

Weekly roundup of Digital Forensics and Incident Response news

ThinkDFIR (2017+)

Personal research blog
Investigation

- The DS-1 Orbital Battle Station has been destroyed
- We have identified the Rebel Base
- Top forensicicators deployed to the scene
- Tasked with providing investigative support
Investigative Questions

Tell us everything you can about these devices!
Investigative Questions

- What access point were the devices connected to?
- Were the devices connected to each other?
- What accounts were they linked to?
- What has the Google Home device heard?
- Current or previously connected Bluetooth devices?
- Any useful location information?
Devices

Google Home Mini
Devices

Google Home Mini

Android device
Devices

Google Home Mini

Android device
Phone Examination
Google Home App

- For device interaction
- No web interface
- com.google.android.apps.chromecast.app
Phone

- Nexus 5 running Android 5
- Home app version: 12827030

- ADB Backup: **X**
- Physical: **✓**
- Tested iOS backup
Findings from Target phone - User Account Details

- Shows all available Google addresses on the device
Findings from Target phone - User Account Details

- Shows all available Google addresses on the device
Investigators Phone

- User’s name and picture but no email
- Name of home device
Findings from Target phone – Linked Home Devices

- Devices on the user account
- Device address (set by user)
Device Address

- com.google.android.apps.chromecast.app_preferences_no_backup.xml
- “Current location” in “My Activity”
- Set by the user, not GPS
Home Graph

- `home_graph_<base64 string of Account email>.proto`
Home Graph

- home_graph_<base64 string of Account email>.proto
Home Graph

- `home_graph_<base64 string of Account email>.proto`
Home Graph

- home_graph_<base64 string of Account email>.proto
Findings from phone

- **Google Account information** & OAuth Token - rebelsonyavin@gmail.com
  100256536036704352743

- **Device Location** - 5858 Lucas Valley Rd, Nicasio

- **Cloud Device ID** - 47E85C43B5D495BE76BF9A9624B1A4A3

- **Wifi password** - starkiller
Google Home Examination

https://www.etsy.com/ie/listing/582594213/death-star-google-home-mini-star-wars
Google Home Examination

- Query the live device
- Examine the internals
Find the Google Home

- IP from Home app
- Network scanner app (eg: Fing)
- Nmap scan
Scanning

Starting Nmap 6.47 ( http://nmap.org ) at 2018-03-05 21:24 AEDT
Nmap scan report for 192.168.0.13
Host is up (0.024s latency).
Not shown: 996 closed ports

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>8008/tcp</td>
<td>open</td>
<td>http</td>
</tr>
<tr>
<td>8009/tcp</td>
<td>open</td>
<td>ajp13</td>
</tr>
<tr>
<td>9000/tcp</td>
<td>open</td>
<td>cslistener</td>
</tr>
<tr>
<td>10001/tcp</td>
<td>open</td>
<td>scp-config</td>
</tr>
</tbody>
</table>

nmap -p 8008,8009,9000,10001 192.168.0.1-255 --open
Query

- Google Home app
- Homespeak.py
Homespeak

- GET/POST Requests → JSON
- Connect to network/device
- Cloud Device ID
- Bluetooth Devices
Putting It Together

Home Graph
Cloud Device ID
Google Account ID
Gmail Address
Putting It Together

Homespeak
Cloud Device ID
Putting It Together

Cloud Device ID

Home Graph
- Cloud Device ID
- Google Account ID
- Gmail Address

Homespeak
- Cloud Device ID
Putting It Together

Cloud Device ID

Google Account
Query - Bluetooth Devices

Paired Bluetooth devices

Lukes Nexus 5
Added 4/4/2018

```
"bond_date": 1522822989797.648,
"connected": false,
"device_class": 5898764,
"device_type": 1,
"last_connect_date": 1522822994064.054,
"mac_address": "48:59:29:61:b3:d0",
"name": "Lukes Nexus 5",
"rssi": -255
```
Query - Bluetooth Devices

"bond_date": 1522822989797.648,
"connected": false,
"device_class": 5898764,
"device_type": 1,
"last_connect_date": 1522822994064.054,
"mac_address": "48:59:29:61:b3:d0",
"name": "Lukes Nexus 5",
"rssi": -255
Google Home Tear Down
Flash Memory

Toshiba TC58NVG1S3HBA16 256 MB NAND flash
Google Home Acquisition

- Rework station to remove chip
- BGA 67 Socket + NAND Flash Chip Reader (Dataman)
Home dump - Strings

- Bluetooth devices
- Google Account ID (GAIA)
Home dump - Strings

- Bluetooth devices
- Google Account ID (GAIA)
Putting It Together

Google app
Cloud Device ID
Google Account ID
Gmail Address

Cloud Device ID
Google Account ID

NAND Read
Google Account ID
Cloud Device ID

Homespeak
Cloud Device ID
Cloud Data Examination
Manual Cloud Acquisition

- Access “My Activity”
  - Filter for “Assistant” and “Voice & Audio”
  - Known users voice
  - Identify that Google Home was used (most of the time, but not which Google Home)

- Google Takeout
  - Spoken words
  - Responses
  - Audio
  - Location if set
Cloud data acquisition tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Version</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAGNET FORENSICS</td>
<td>AXIOM</td>
<td>V1.2.6</td>
</tr>
<tr>
<td>Oxygen Forensics</td>
<td>Detective</td>
<td>V10.2</td>
</tr>
<tr>
<td>Cellebrite</td>
<td>Cloud Analyzer</td>
<td>V7.1</td>
</tr>
<tr>
<td>Google</td>
<td>Takeout/My Activity</td>
<td>April 2018</td>
</tr>
</tbody>
</table>
Cloud Data Findings

- Asked what the plan was for the day

Assistant

Said do I have anything coming up on my calendar
Apr 4, 2018, 4:24:10 PM

Products:
Assistant

Locations:
From your current location: https://google.com/maps?q=38.064384,-122.646286

Details:
Started by hotword
Cloud Data Findings

Blow up the Death Star

Wednesday, Apr 4, 2018
rebels yavin
Cloud Data Findings

- Query for “What's the weather like on Hoth”

Assistant

Said what's the weather like on Hoth
Hoth's climate is Cold.
Apr 4, 2018, 4:25:42 PM

Products:
   Assistant

Locations:
   From your current location: https://google.com/maps?q=38.064384,-122.646286

Details:
   Started by hotword
Generalised Process
General Process

- Physical acquisition of Android phone
- Identify Google Account and Cloud ID from Home Graph
- Query home device to get Cloud ID and Bluetooth data
- Pull the cloud data
Overall Findings
Overall Findings

- The room most likely related to someone named Luke
- He had a calendar entry to destroy our Imperial pride
- Home location set to Skywalker Ranch - could be previous location
- Potential last Date/time at the base based on bluetooth connection
- He was asking about the weather on Hoth.
Further Work

- Parse Google Home file system
- Further decoding of the proto file
- iOS app examination
- Calling feature – not available in Australia to test
- Future units may have cameras/displays
Thanks

All the companies that gave me access to their software for this testing: Magnet Forensics, Cellebrite, Oxygen, Paraben, Compelson, MSAB

Jessica Hyde
Steve Watson
Robert Fearn
Scott Lalliss
David Cowen
Questions

@phillmoore
randomaccess3@gmail.com
Thisweekin4n6.com
ThinkDFIR.com
Github.com/randomaccess3