Hunting PBX

For Vulnerabilities
Sachin Wagh
Security Analyst

- Security Intelligence Team @ Symantec
- Speaker at Hakon and Geek Street - Infosecurity Europe
- Bug Hunter | Penetration Tester
- Security Blogger

@tiger_tigerboy
Himanshu Mehta
Senior Threat Analysis Engineer

✓ Security Intelligence Team @ Symantec
✓ Speaker at National Cyber Security Conference, Hakon & Geek Street - Infosecurity Europe
✓ Advisory Board Member @EC-Council & Convetit
✓ Bug Hunter | Penetration Tester

@LionHeartRoxx
Content

• What is PBX
• Features
• Searching
• Softphone
• Vulnerabilities
• Mitigations
Private Branch Exchange

Hunting PBX for Vulnerabilities

Source: http://www.cealcomz.co.za
Features

• Call Forwarding
• Call Transfer
• Conference Calls
• Automatic Call Delivery (ACD)
• Voice Messaging
• Call Queue ..etc
Hunting PBX for Vulnerabilities
Call Details Records

Hunting PBX for Vulnerabilities
Censys: "FreePBX Administration"
Censys: "FreePBX Administration"

Query Metadata

Your query ("FreePBX Administration") found 12,273 IPv4 hosts.

Country Breakdown

<table>
<thead>
<tr>
<th>Country</th>
<th>Hosts</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>5,518</td>
<td>44.96%</td>
</tr>
<tr>
<td>Canada</td>
<td>789</td>
<td>6.43%</td>
</tr>
<tr>
<td>Russia</td>
<td>633</td>
<td>5.16%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>415</td>
<td>3.38%</td>
</tr>
<tr>
<td>Italy</td>
<td>400</td>
<td>3.26%</td>
</tr>
<tr>
<td>Brazil</td>
<td>352</td>
<td>2.87%</td>
</tr>
<tr>
<td>Germany</td>
<td>327</td>
<td>2.66%</td>
</tr>
<tr>
<td>France</td>
<td>308</td>
<td>2.51%</td>
</tr>
<tr>
<td>Ukraine</td>
<td>225</td>
<td>1.83%</td>
</tr>
<tr>
<td>Netherlands</td>
<td>181</td>
<td>1.47%</td>
</tr>
</tbody>
</table>

Network Breakdown

<table>
<thead>
<tr>
<th>Autonomous System (AS)</th>
<th>Hosts</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBERLYNK - Wisconsin CyberLynk Network, Inc., US</td>
<td>604</td>
<td>4.92%</td>
</tr>
<tr>
<td>AS-HOOPA - Choope, LLC, US</td>
<td>498</td>
<td>4.06%</td>
</tr>
<tr>
<td>AMAZON-NO - Amazon.com, Inc., US</td>
<td>432</td>
<td>3.52%</td>
</tr>
<tr>
<td>OVH, FR</td>
<td>414</td>
<td>3.37%</td>
</tr>
<tr>
<td>DIGITALOCEAN-ASIN - DigitalOcean, LLC, US</td>
<td>402</td>
<td>3.28%</td>
</tr>
<tr>
<td>AMAZON-AES - Amazon.com, Inc., US</td>
<td>366</td>
<td>2.98%</td>
</tr>
<tr>
<td>COMCAST-9122 - Comcast Cable Communications, LLC, US</td>
<td>339</td>
<td>2.76%</td>
</tr>
<tr>
<td>GOOGLE - Google LLC, US</td>
<td>149</td>
<td>1.21%</td>
</tr>
<tr>
<td>LINODE-AP Linode, LLC, US</td>
<td>121</td>
<td>0.99%</td>
</tr>
<tr>
<td>CYBERLYNK-PHOX - Wisconsin CyberLynk Network, Inc., US</td>
<td>119</td>
<td>0.97%</td>
</tr>
</tbody>
</table>

Hunting PBX for Vulnerabilities
Hunting PBX for Vulnerabilities
Hunting PBX for Vulnerabilities

Shodan: “polycom+command+shell”
### File Transfer Protocol (FTP)

#### Index of /incoming/

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Date Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>1kbtst.pdf</td>
<td>1.020B</td>
<td>2/6/16, 5:30:00 AM</td>
</tr>
<tr>
<td>GXHLGSL.txt</td>
<td>4 B</td>
<td>7/15/17, 5:30:00 AM</td>
</tr>
<tr>
<td>H251418357.txt</td>
<td>2.0 kB</td>
<td>8/6/17, 5:30:00 AM</td>
</tr>
<tr>
<td>IMG001.exe</td>
<td>3.4 MB</td>
<td>9/24/16, 5:30:00 AM</td>
</tr>
<tr>
<td>M216631837.txt</td>
<td>2.0 kB</td>
<td>8/6/17, 5:30:00 AM</td>
</tr>
<tr>
<td>PBX_Test.txt</td>
<td>28 B</td>
<td>6/15/18, 7:40:00 PM</td>
</tr>
<tr>
<td>Photo.scr</td>
<td>1.5 MB</td>
<td>2/6/16, 5:30:00 AM</td>
</tr>
<tr>
<td>ascii.txt</td>
<td>132 B</td>
<td>6/14/18, 11:29:00 PM</td>
</tr>
<tr>
<td>auumxyaq.txt</td>
<td>9 B</td>
<td>5/17/16, 5:30:00 AM</td>
</tr>
<tr>
<td>auofpido.txt</td>
<td>9 B</td>
<td>1/24/16, 5:30:00 AM</td>
</tr>
<tr>
<td>biofztys.txt</td>
<td>9 B</td>
<td>3/19/16, 5:30:00 AM</td>
</tr>
<tr>
<td>bzegoxzm.txt</td>
<td>9 B</td>
<td>3/7/16, 5:30:00 AM</td>
</tr>
<tr>
<td>bzkqftqyn.txt</td>
<td>9 B</td>
<td>1/22/16, 5:30:00 AM</td>
</tr>
</tbody>
</table>

**Hunting PBX for Vulnerabilities**
### Call Detail Record - Search Returned 100 of 350 Calls

<table>
<thead>
<tr>
<th>Call Date</th>
<th>File</th>
<th>Source</th>
<th>Destination</th>
<th>Application</th>
<th>Src Channel</th>
<th>Dst Channel</th>
<th>Disposition</th>
<th>Duration</th>
<th>BillSec</th>
<th>Userfield</th>
<th>Account</th>
<th>&quot;Listen to call recording&quot;</th>
<th>&quot;Play Recording&quot;</th>
</tr>
</thead>
</table>

**Hunting PBX for Vulnerabilities**
Hunting PBX for Vulnerabilities

```
root@tigerboy:~# smbclient \\192.168.1.200\\tmp
Enter root's password:
Anonymous login successful
Domain=[PBX] OS=[Unix] Server=[Samba 3.0.23c-2]
smb: \> ls

  .  VMwareTools-
  ..  0.1.6-5214329.
  .cron_output_backup.log N 673692 Sat Jun 16 17:15:02 2018
  4437_7460 D 0 Sun Nov 5 08:05:24 2006
  .font-unix
  .ICE-unix
  backup-config-manifests D 0 Sat Jun 16 12:00:05 2018
  cron_output_ftp_backup.log N 88 Sat Jun 16 12:30:02 2018
  4354_13022 D 0 Tue Aug 16 03:38:28 2015
  4399_24753 D 0 Tue Aug 16 07:08:56 2016
  4406_3627 D 0 Tue Aug 16 02:49:12 2015
  4387_9307 N 88 Sat Jun 16 12:30:02 2018
  .webmin
  cron_output_websync.log N 3502 Sat Jun 16 12:30:36 2018
  cron_output_updatedirectory.log N 351 Sat Jun 16 12:30:32 2018
  sftpLocalSocket A 0 Mon Aug 18 15:04:18 2014
  4370_15876 DR 0 Tue Aug 16 03:29:50 2016
  4397_16519 DR 0 Tue Aug 16 02:37:12 2015
  4365_36648 DR 0 Tue Aug 16 03:64:19 2015
  4357_22757 DR 0 Tue Aug 16 03:49:18 2015
  4381_226 DR 0 Tue Aug 16 05:34:58 2016
  cron_output_spool.log N 3200 Sat Jun 16 12:30:39 2018
  4401_24170 DR 0 Tue Aug 16 03:21:55 2016
  cron_output_tftppboot.log N 262 Sat Jun 16 12:30:08 2018
```
Server Message Block (smb)

Hunting PBX for Vulnerabilities
Shodan: “port:23 console gateway -password”
Vulnerabilities

Hunting PBX for Vulnerabilities
Blind OS Command Injection

I AM NOT BLIND
I'VE JUST SEEN ENOUGH

Hunting PBX for Vulnerabilities
Blind OS Command Injection [DEMO]
Path Traversal [DEMO]

CVE-2017-14537
Path Traversal [DEMO]

Hunting PBX for Vulnerabilities

CVE-2017-14537
Cross-site Scripting

source:gif-finder.com

Hunting PBX for Vulnerabilities

XSS EVERWHERE
Cross-site Scripting [DEMO]

CVE-2017-14536
Cross-site Scripting [DEMO]

CVE-2018-11552
Local Code Execution

Hunting PBX for Vulnerabilities
Local Code Execution [DEMO]

CVE-2018-11551
Hunting PBX for Vulnerabilities
Local Code Execution [DEMO]
Hunting PBX for Vulnerabilities
Mitigations

- **POLICIES AND PROCEDURES:**
  - SECURITY TRAINING
  - PASSWORD POLICY
  - INCIDENT RESPONSE PROCEDURE

- **OS LEVEL SECURITY:**
  - PATCHES
  - APPLICATIONS AND SERVICES
  - PRIVILEGES
Thank You