War Dialing Part 1: The VoIP and Analog Primer

November 10, 2014

War Dialing Part 1: The VoIP and Analog Primer

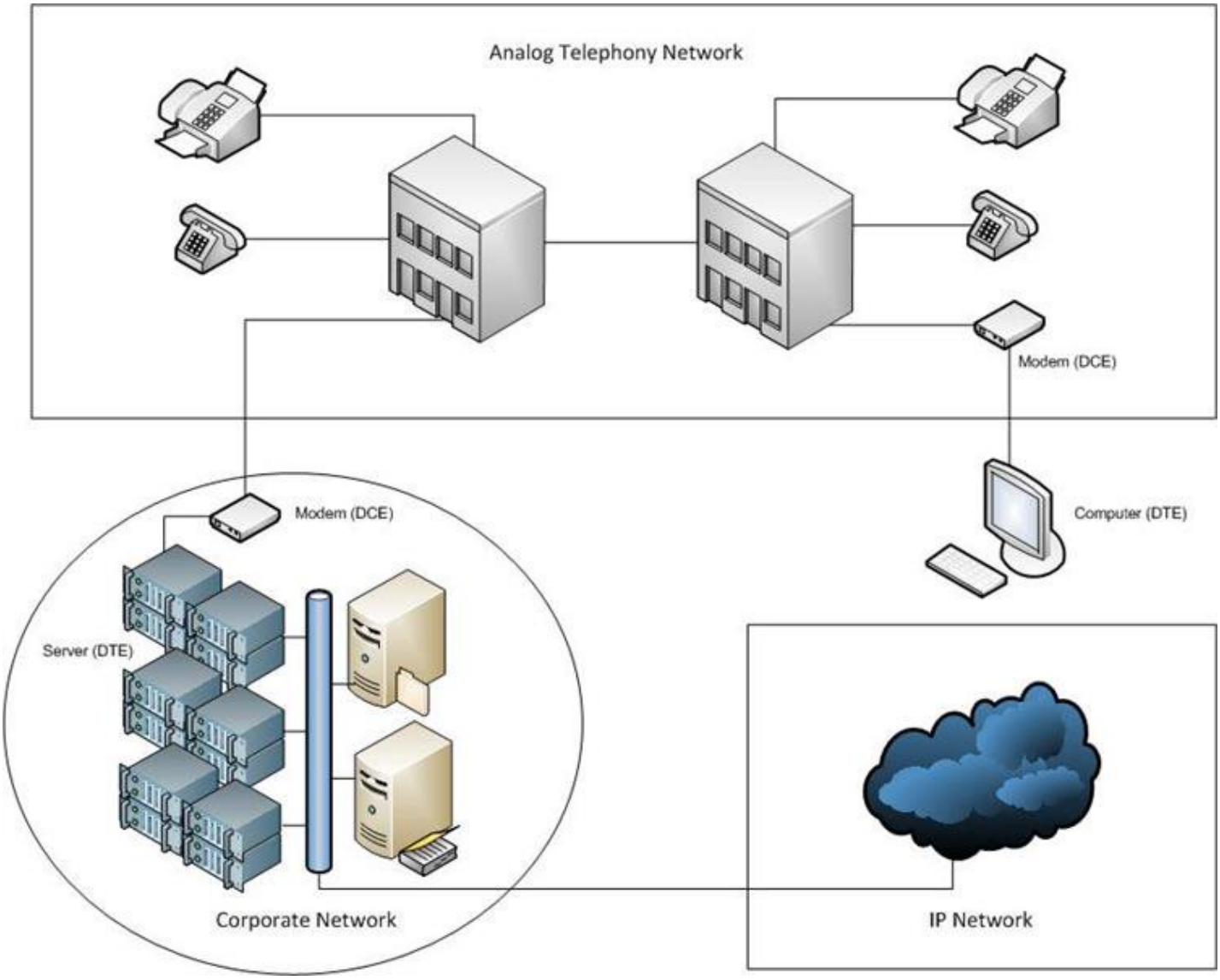
In this series of posts, I will introduce the concept of telephony war dialing along with techniques to perform such assessments. Initially, we need to describe "war dialing" and its practical application. In order to serve this justice, we need a short history lesson on telephony.

Decades ago, prior to the ever ubiquitous Voice over IP (VoIP) bundles provided by megalithic companies such as Verizon or Time Warner, we had American Telephone and Telegraph (AT&T). AT&T had a monopolistic reach on the analog telephone circuit

switched network. As such, everything was interconnected via central offices, tandems and switches such as the Crossbar. Essentially, voice communications were interconnected geographically, similar to how we route data packets in modern day.

However, voice was not the only payload transmitted across the analog wire, so was data. Organizations leveraged what was referred to as Data Conditioning Equipment (DCE) in order to connect and communicate with Data Terminal Equipment (DTE). This can be thought of as synonymous with our cable routers (DCE) connected to our computers (DTE).

Specifically, the DCE devices - in this case we are referring to modems - were tied to an endpoint that was associated with a particular landline phone number. Two modems, one sender and one receiver could negotiate baud rate and establish a data transaction. Modems can be considered connected nodes on a network; albeit, the external access network is different than the internal connected network. Modems are typically connected via existing analog landlines and are often used as a method to gain access to a system and/or network using out-of-band access in the event that traditional IP packet switched networks become unavailable. The following illustration provides a high-level depiction of an analog network and an IP-based network. It's also the point in which both transport methods converge within a central network, such as a corporate datacenter or enterprise network.



The term "war dialing" is used to describe the technique of auto-dialing phone blocks, disparate or contiguous ranges, in an attempt to locate available modems such as the ones located in the corporate network on the previous illustration. The modems are then inspected for insecure configurations in an attempt to gain access to the target system and/or network. This is something that we do quite often at FishNet Security as a standalone service or in conjunction with blended assessments, such as our Breach Assessment. Let's get to how we war dial when we have VoIP and analog networks to contend with.

The following list of components will be used to set up our war dialing environment. Since it is becoming very rare to actually have a native analog line at our disposal, we are going to shovel packets across a VoIP transport; more about this later.

- A dialing device capable of dialing large phone number ranges
- A device for performing tone detection via a digital signaling processor (DSP)

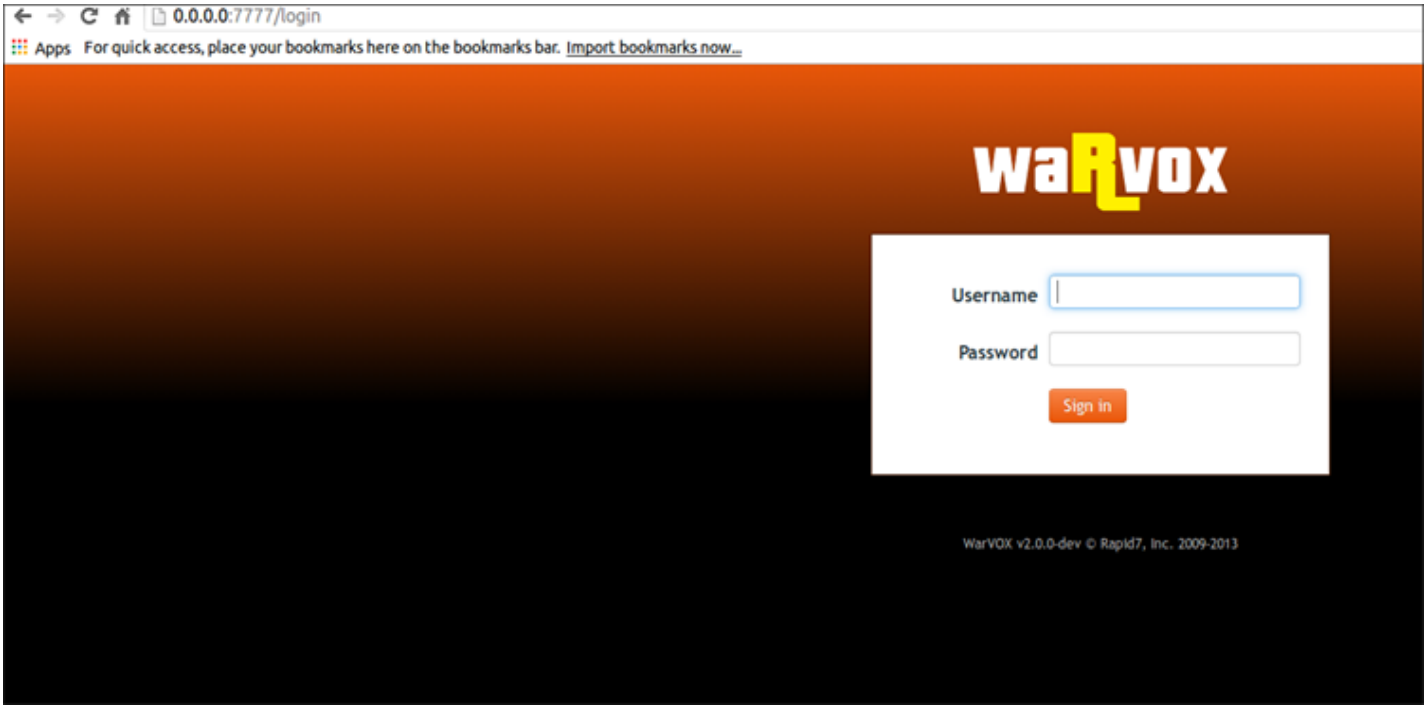
- A method to extrapolate the results
- A method to validate the modems phone number ownership details
- A carrier grade modem suitable for interacting with our detected modems
- A device to convert from sine to block encoding so we can interact via VoIP transport
- A program suitable for manual interaction with the target modem device

Mass Dialing and Tone Detection

In order to prevent dialing each number manually, we need to use an auto-dialer. Luckily, HD Moore created a very effective utility called Warvox2. This is the successor to Warvox and adds some nice features, such as a custom IAX library and PostgreSQL database storage. Additionally, it allows for a fully featured Digital Signaling Processor, using the Kiss FFT library, in order to perform audio and frequency analysis. First we need to grab Warvox2 from the GitHub location, https://github.com/rapid7/warvox/ (https://github.com/rapid7/warvox/). The GitHub site claims that the following “install process is not ideal at the moment”; however, it works well and is really straight forward.

```
$ sudo apt-get install gnuplot lame build-essential libssl-dev libcurl-openssl-dev \
  postgresql postgresql-contrib git-core curl
Install RVM to obtain Ruby 1.9.3 or later

$ \curl -L https://get.rvm.io | bash -s stable --autolibs=3 --rails
Clone this repository to the location you want to install WarVOX:

$ git clone git://github.com/rapid7/warvox.git /home/warvox
Configure WarVOX:

$ cd /home/warvox
$ make
Configure the PostgreSQL account for WarVOX:

$ sudo su - postgres
$ createuser warvox
$ createdb warvox -O warvox
$ psql
psql> alter user warvox with password 'randompass';
psql> exit
Copy the example database configuration to database.yml:

$ cp config/database.yml.example config/database.yml
Modify config/database.yml to include the password set previously

Initialize the WarVOX database:

$ make database
Add an admin account to WarVOX

$ bin/adduser admin
Start the WarVOX daemons:

$ bin/warvox.rb
Access the web interface at http://127.0.0.1:7777/
```

As the installation states, we should be able to reach the web server at 127.0.0.1 on port 7777.



Initial Warvox2 authentication page

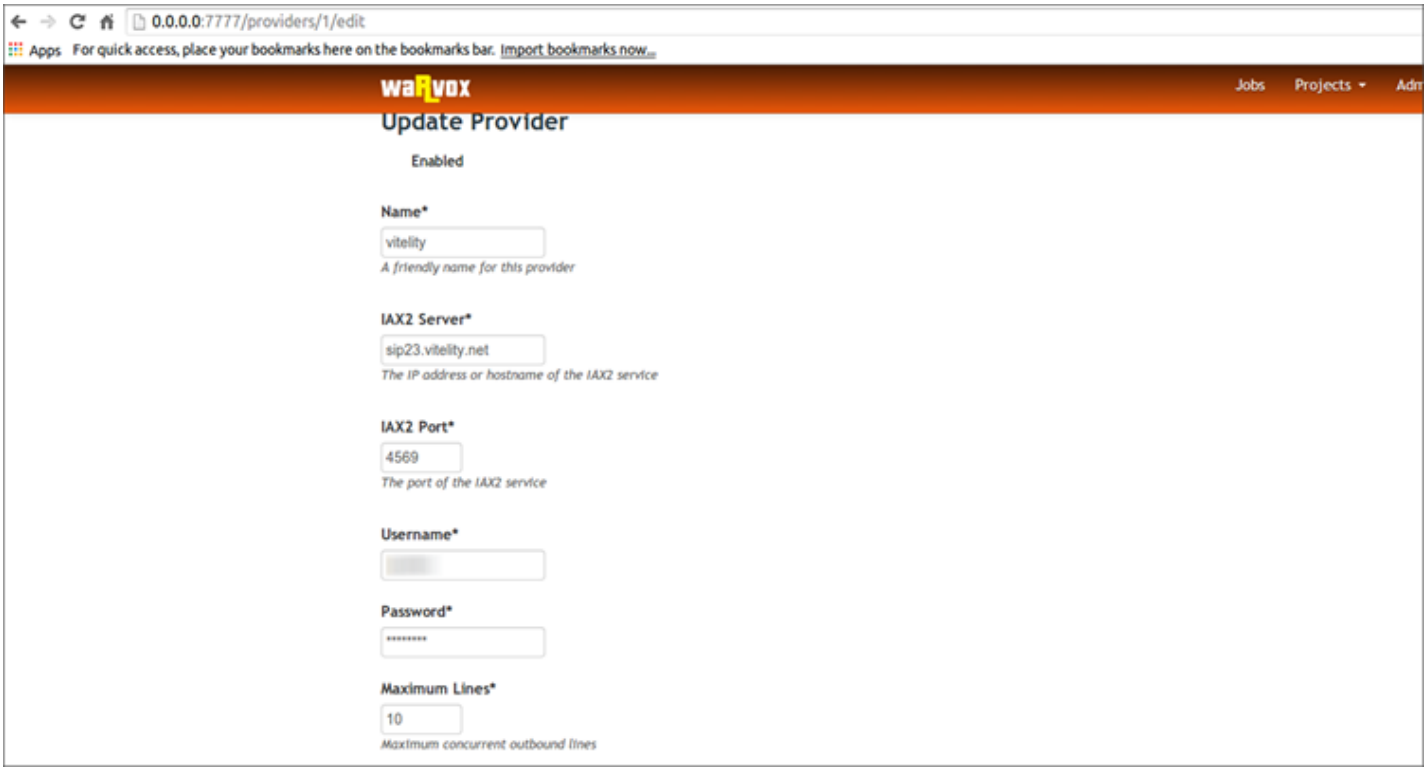
Warvox2 binds to the 127.0.0.1 interface; however, in order to connect remotely, we need to modify the "bin/warvox.rb" code. Easy enough just change the lines similar to the following:

```
opts    =
{
        'ServerPort' => 7777,
        'ServerHost' => '0.0.0.0',
        'Background' => false,
}
```

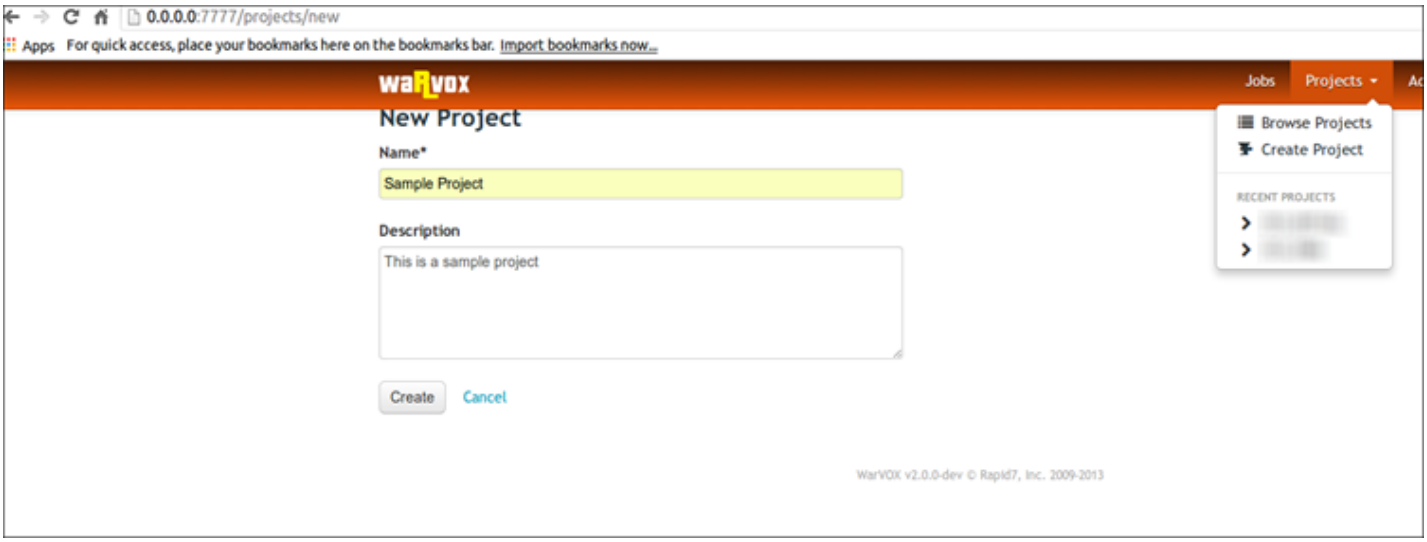
Warvox2 server configuration code block

I have an internal system in which I don't care if Warvox2 is bound to all the interfaces, so I enter 0.0.0.0 in order to do so. Alternatively, the IP of the interface is probably more appropriate here.

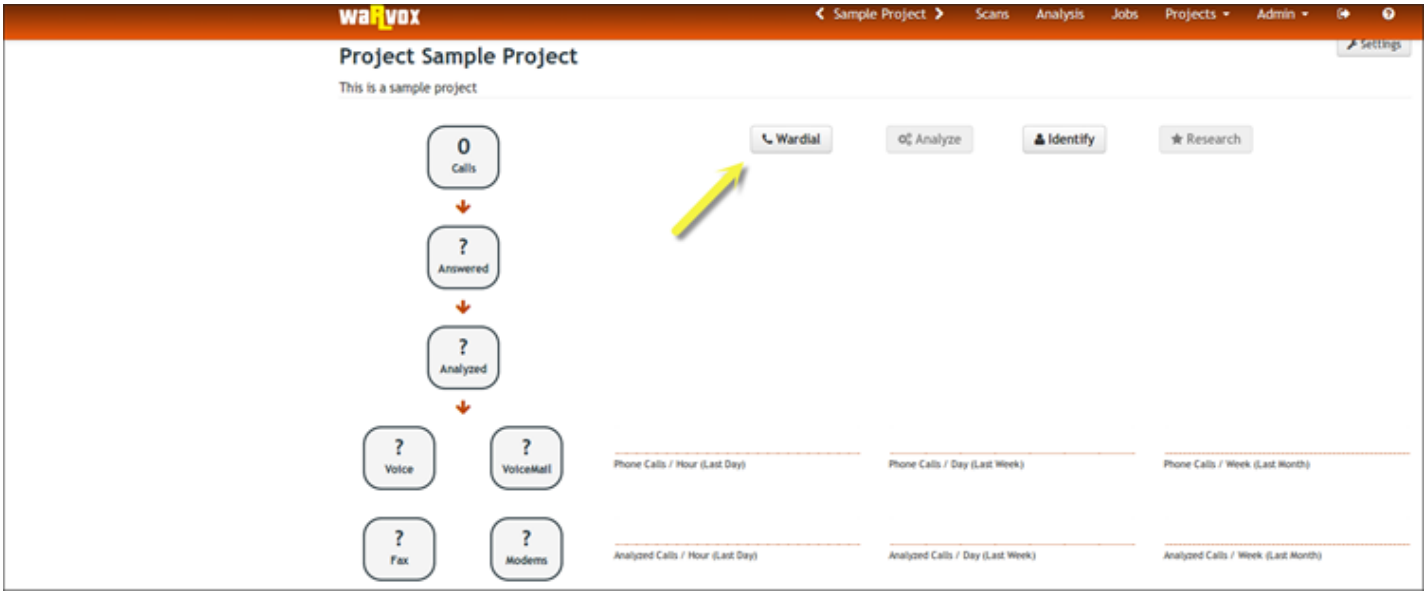
With that done, let's navigate the application. First, we need to add a service provider. Warvox2 is intended to be used with an IAX protocol service provider. A couple of well-known service providers exist and offer "pay as you go" plans. The first is Vitelity, although, their IAX protocol support is undocumented, and they prefer to run native SIP trunks. The second is Teliax who offers native IAX protocol support. I personally use both and don't have any issues with either.



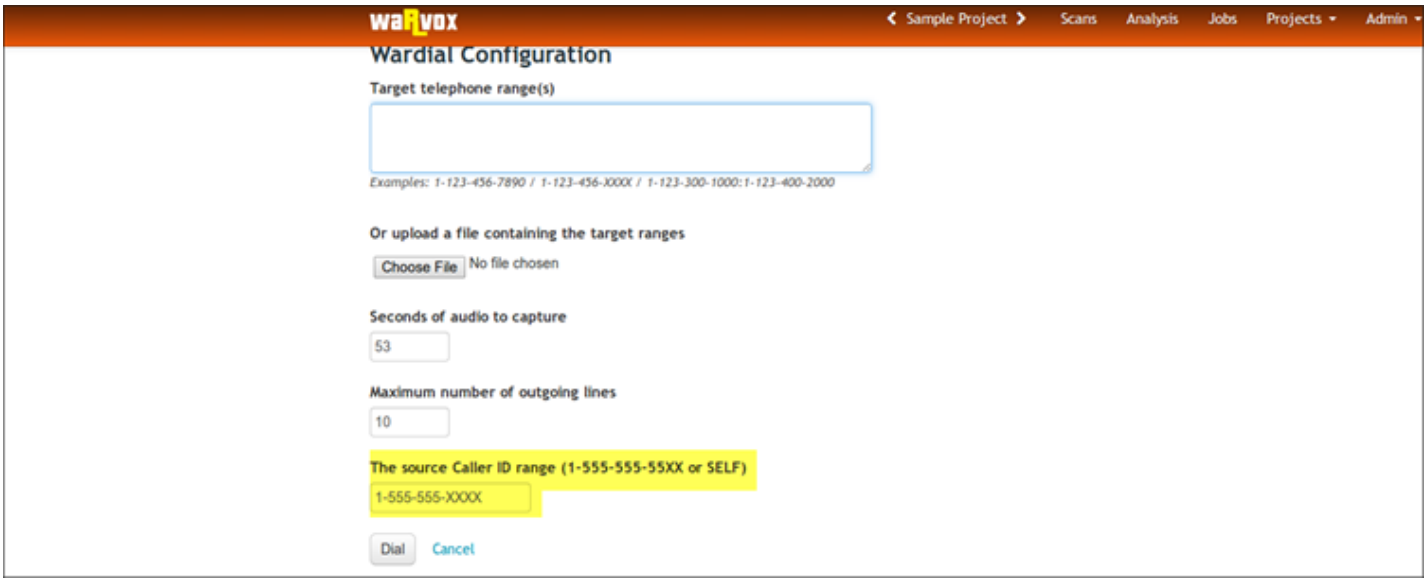
Insert the SIP provider details, whether that is Vitelity or Teliax



Create a project that will become the workflow



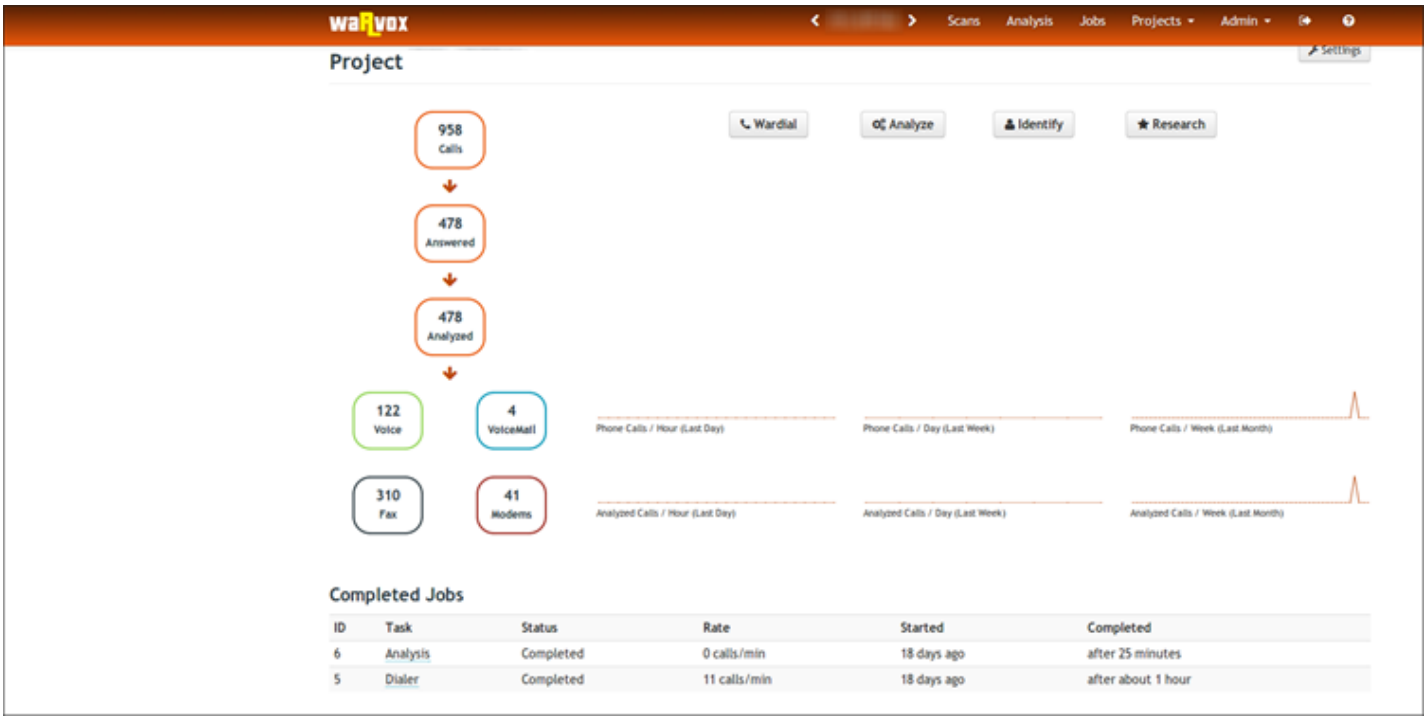
The wardial button will be used to enter job details



Phone range entry and call-specific details

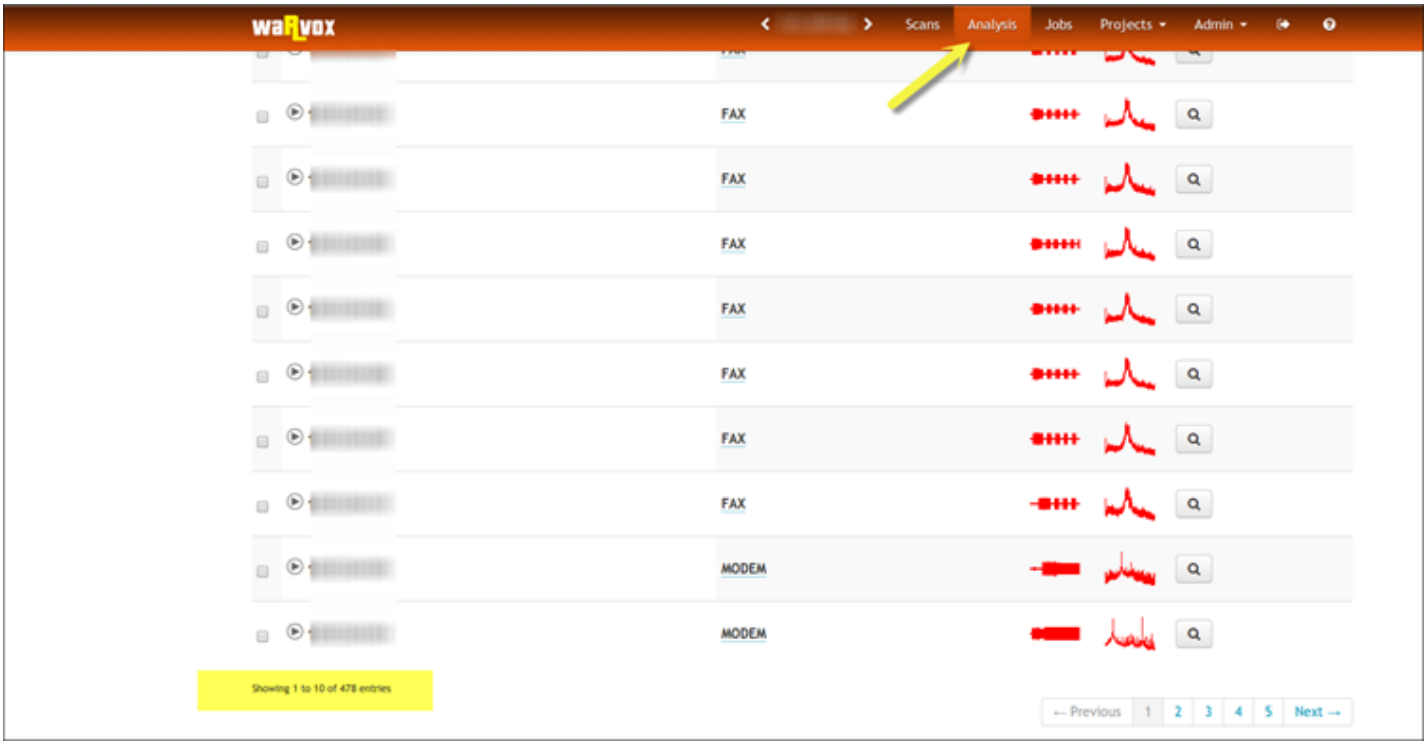
Note that the preceding illustration has a highlighted area that allows for the source Caller ID description. This can be a phone number of your choosing as both Vitelity and Teliax pass this number through on their IAX trunks and will appear on the recipient's caller ID. However, "SELF," if set instead of a number, will force the phone number being dialed to also be set as the source caller ID variable. This is important because some voicemail boxes will fail to open without requiring pin/password authentication, because it is assumed that the person is accessing their voicemail from their phone, locally. Set the SELF option; it still works, and we run into voicemail access quite often.

Now we need to dial the numbers. We should see something similar to the following. Note that this is a project that was already analyzed hence the reason why the "analyzed" tones are included in the screenshot.



The call progress and workflow details

Now if we click on the "Analysis" button within the navigation bar, we should see something similar to the following:



Analyzed calls, tone detection and resulting audio

Alright, so the analysis can take some time, so grab a Snickers and some Hi-Ball because Warvox2 has to run 53 seconds of audio capture multiplied by the number of phone numbers within the phone block and compare it to known audio patterns. There is a lot more to this process, and HD Moore has an excellent presentation titled Acoustic Intrusions (http://www.irongeek.com/i.php?page=videos/derbycon1/keynote-hd-moore-acoustic-intrusions) on the topic that was delivered at the 2011 DerbyCon.

Another problem that can be a bit time consuming is obtaining the results of the analysis without paginating through a seemingly infinite collection of pages. We'll cover that in the next installment.

By: Chris Patten (/blog/author/chris-patten)

Share:

How Can We Help?

Let us know what you need, and we will have an Optiv professional contact you shortly.

Company Email

First Name

Last Name

Company Name

Work Phone

Country

Select...

How can we help?

Additional Information

Select...

By checking this box, you consent to Optiv using the information you provided to subscribe you to communications and content from Optiv and its partners (https://www.optiv.com/security-solutions/security-technology/partner-directory?keys=&sort=az) relevant to your request. Such communications may be in the form of email, phone, or postal service. You may unsubscribe at any time. Optiv respects your privacy: for additional details on how Optiv uses and protects your information, click here (https://www.optiv.com/privacy-policy) to view our Privacy Policy.

☐

Submit

RELATED INSIGHTS

(/explore-optiv-insights/downloads/endpoint-security-assessment)

December 15, 2017

Endpoint Security Assessment (/explore-optiv-insights/downloads/endpoint-security-assessment)

Optiv can help validate the effectiveness of your endpoint security solution by identifying and exploiting vulnerabilities.

See Details (/explore-optiv-insights/downloads/endpoint-security-assessment)

Stay in the Know

For all the latest cybersecurity and Optiv news, subscribe to our blog and connect with us on Social.

Subscribe

(https://www.linkedin.com/company/optiv-inc/) (https://twitter.com/Optiv)
(https://www.facebook.com/OptivInc/) (https://www.instagram.com/optivsecurity/)
(https://www.youtube.com/c/OptivInc)

Join Our Email List

We take your privacy seriously and promise never to share your email with anyone.

Company Email

By checking this box, you consent to Optiv using the information you provided to subscribe you to communications and content from Optiv and its partners (https://www.optiv.com/security-solutions/security-technology/partner-directory?keys=&sort=az) relevant to your request. Such communications may be in the form of email, phone, or postal service. You may unsubscribe at any time. Optiv respects your privacy: for additional details on how Optiv uses and protects your information, click here (https://www.optiv.com/privacy-policy) to view our Privacy Policy.

Submit

Stay Connected

Find cybersecurity Events in your area. (/our-story/events)

(/our-story/events)

SECURITY SOLUTIONS (/SECURITY-SOLUTIONS)

PARTNER DIRECTORY (/PARTNER-DIRECTORY)

EXPLORE OPTIV INSIGHTS (/EXPLORE-OPTIV-INSIGHTS)

OUR STORY (/OUR-STORY)

JOIN OPTIV TEAM (/JOIN-OPTIV-TEAM/CAREERS)

CLIENT PORTAL (HTTP://CLIENT.OPTIV.COM)

(https://www.linkedin.com/company/optiv-inc/) **(https://twitter.com/Optiv)**

(https://www.facebook.com/OptivInc/) **(https://www.instagram.com/optivsecurity/)**

(https://www.youtube.com/channel/UC5dqDQ0tLgaohPd9meSCB6g)

Home (/) | **Contact (/contact-us)** | **Cookie Policy (/optiv-cookie-policy)** | **Privacy Policy (/privacy-policy)** | **Terms of Use (/terms-of-use)** | **Sitemap (/sitemap)**