System Shock: The Shodan computer search engine

I’m Viss. I do security research.

I’ve presented at:
Defcon/BlackHat/ToorCon(s)/BSides/BarCamp/OWASP/HITB
Time for some RESPECT.

I am here because of someone else's misfortune.

It's great for me, but horrible for them.

I just want to acknowledge that.
Credentials:

- Aaaaaahahahahahahaha
- HHAHAHAhahahahAHAhaha!
- omg rofl lolz hahaha seriously
- I can’t seriously do this slide with a straight face
- I read an nmap book once
- I totally stole this idea from zfasel and I owe him booze for it.
- my CISSP code of ethics mandates I report you
Who here has NOT heard of Shodan?
Who here knows what TCP Banners are?
Any python coders in here?

You guys are gonna love this :D
Shodan is like google but for tcp banners.

It also has a python API

You can bridge that API to tools

... like metasploit. Or armitage and cortana

Or you can just screenshot the entire net
Find an interesting query.

Believe me - there is enough absurdity on the internet - its VERY EASY TO FIND.

2-3 steps of refinement = goldmines
My first forray into this: TONS AND TONS OF WEBCAMS.
Webcams! .. speaking of goldmines..
Who watches the watchers?
Who watches the watchers?

Meeeeeeee >:D
Now for more meta

a camera in the business that makes the cameras, watching people MAKE THE CAMERAS I’m watching them with
Scada gear on webcams!
Other stuff on webcams!
But most cameras are boring
This thing!

... (no idea)
A um.. “T-2000”! ..

... what's a T-2000?.. relion?
Its a hydrogen fuel cell.
Relion’s modular cartridge approach normally operates with six cartridges connected to a common BUS. Each cartridge supplies a nominal power of 200W.

In case a cartridge is damaged, the replacement procedure can be performed in a few seconds while the fuel cell continues to provide power to the load.

- Figure 2 – Relion’s T-1000 hydrogen fuel cell
Gets used a lot in .mil...

## DOE/DOD Back-Up Power Demonstration

<table>
<thead>
<tr>
<th>Site</th>
<th>kW Req'd</th>
<th>Buildings Backed-up</th>
<th>Fuel Cell Units Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aberdeen Proving Ground</td>
<td>15, 20, 8</td>
<td>Energy Management Building, Range Control and Coordination, DPW Conservation Branch</td>
<td>3 IdaTech ElectraGen 5; Hyrogenics HyPM Rack 20; RelIon T-2000 8kW</td>
</tr>
<tr>
<td>Fort Bragg</td>
<td>15</td>
<td>Training Range Control Building</td>
<td>3 IdaTech ElectraGen 5</td>
</tr>
<tr>
<td>Picatinny Arsenal</td>
<td>10, 10</td>
<td>Sewage Lift Pump, Sewage Lift Pump</td>
<td>2 IdaTech ElectraGen 5; 2 IdaTech ElectraGen 5</td>
</tr>
<tr>
<td>West Point</td>
<td>20, 20</td>
<td>Internet Switch, Internet Service and Telecom Closet</td>
<td>Altery FPP-20; Altery FPP-20</td>
</tr>
<tr>
<td>Cheyenne Mountain</td>
<td>24</td>
<td>911 Call Center</td>
<td>RelIon T-2000 4kW, 8kW, 12kW</td>
</tr>
<tr>
<td>Fort Hood</td>
<td>8, 10</td>
<td>Wastewater Pretreatment Plant, Wastewater Pretreatment Plant</td>
<td>RelIon T-2000 8kW, RelIon T-1000 1.2 kW; Altery FPP - 10</td>
</tr>
<tr>
<td>Marines 29 Palms</td>
<td>4</td>
<td>Internet Switch</td>
<td>RelIon T-2000 4kW</td>
</tr>
</tbody>
</table>
This is how you use it
So where do you find these things in meatspace?
Oh..
Wind farms!

---

Image of a wind farm monitoring screen showing real-time and cumulative energy data.
Lighting, HVAC, Alarms
More hvac/lighting
Power meters?
Heat pumps
Bigger heat pumps
REALLY REALLY big heat pumps
Private residences?!
... with trending data?!
Water heaters

Solar System Monitoring

Panel Temp is 55.01 °F

Solar Tank

Outlet Temp is 25.5 °F

Tank Temp is 65.7 °F

Outlet Temp is 75.4 °F

SCP-1 is Off

SCP-2 is Off

Outlet Temp is 30.4 °F

Inlet Temp is 74.3 °F

Valve is 85.5 % Open

DHW Tank

Outlet Temp is 133.6 °F

Outlet Temp is 240.3 °F

DHWMP-1 is On

Thursday, April 11, 13
Familiar displays!
Larger industrial systems
Contents under pressure
Overall, security is a joke.
Overall, security is a joke.
So what can one do with these sorts of findings?

It’s like a fountain of information disclosure.
Level One:

Simple recon
What details can we see?
Quick observations..

[Image of a weather application interface showing temperature and location details along with various checks like PageRank, Rank, Google Trends, McAfee SiteAdvisor, WOT: Trust Worthiness, Vendor Reliability, Privacy, Child Safety, and options.]
We’ve got their scent!
They smell all the way to google maps!
Level Two:

Interactions
DISCLAIMER:

I didn’t have any idea this happened until someone showed me a gallery of screencaps...
Simple social engineering
Massive coolers
Massive coolers with details!
Some scada keeps logs!

<table>
<thead>
<tr>
<th>Date</th>
<th>User</th>
<th>Action</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>13-Apr-12 7:16:15 AM MDT</td>
<td>fox</td>
<td>Opened</td>
<td>165 &lt;- 0 :: WbApplet [guest] @ Owner-PC</td>
</tr>
<tr>
<td>13-Apr-12 7:23:07 AM MDT</td>
<td>fox</td>
<td>Opened</td>
<td>166 &lt;- 0 :: WbApplet [admin] @ Denniss-MacBook-Pro.local</td>
</tr>
<tr>
<td>13-Apr-12 7:24:40 AM MDT</td>
<td>fox</td>
<td>Opened</td>
<td>167 &lt;- 0 :: WbApplet [admin] @ Denniss-MacBook-Pro.local</td>
</tr>
<tr>
<td>13-Apr-12 7:25:19 AM MDT</td>
<td>fox</td>
<td>Closed</td>
<td>166 &lt;- 0 :: WbApplet [admin] @ Denniss-MacBook-Pro.local</td>
</tr>
<tr>
<td>13-Apr-12 7:28:09 AM MDT</td>
<td>fox</td>
<td>Closed</td>
<td>167 &lt;- 0 :: WbApplet [admin] @ Denniss-MacBook-Pro.local</td>
</tr>
<tr>
<td>13-Apr-12 7:31:53 AM MDT</td>
<td>fox</td>
<td>Closed</td>
<td>165 &lt;- 0 :: WbApplet [guest] @ Owner-PC</td>
</tr>
<tr>
<td>13-Apr-12 7:31:54 AM MDT</td>
<td>fox</td>
<td>Opened</td>
<td>168 &lt;- 1 :: WbApplet [guest] @ Owner-PC</td>
</tr>
<tr>
<td>13-Apr-12 7:56:51 AM MDT</td>
<td>fox</td>
<td>Closed</td>
<td>168 &lt;- 1 :: WbApplet [guest] @ Owner-PC</td>
</tr>
<tr>
<td>13-Apr-12 9:19:37 AM MDT</td>
<td>fox</td>
<td>Opened</td>
<td>169 &lt;- 0 :: WbApplet [admin] @ Denniss-MacBook-Pro.local</td>
</tr>
<tr>
<td>13-Apr-12 9:22:55 AM MDT</td>
<td>fox</td>
<td>Closed</td>
<td>169 &lt;- 0 :: WbApplet [admin] @ Denniss-MacBook-Pro.local</td>
</tr>
<tr>
<td>13-Apr-12 9:24:02 AM MDT</td>
<td>sys</td>
<td>Saving station</td>
<td></td>
</tr>
<tr>
<td>13-Apr-12 9:24:04 AM MDT</td>
<td>history.db</td>
<td>Saved history archive</td>
<td>(494ms)</td>
</tr>
</tbody>
</table>
Massive power/UPS gear.
VNC Touchpanels
Level Three:

Stuff that can be abused and is actually kind of scary
Lonworks devices
Its stackable! Like devo hats!
Great Hall is a heated limträsbuehal, with more than 6,000 square meters of DIN-approved sport linoleum brand BoFlex and a further 3,000 square meters of concrete floor. Great Hall is based on a flexible system of props, mobile telescopic grandstands and other facilities that make the hall suitable for virtually all types of events.
Welcome to Hedebo Strandcamping

Directly by the child-friendly sandy beach with blue flag
Our place has something for you if you bring your boat, want to fish like to swim, want to surf, want to sunbathe on the beach, loves long walks in nature or perhaps just want to sit on the bench down at havbakken and enjoy the view above sea level.
Skallerup offers over 262 stylish year-end holiday cottages, divided into 8 different types. You can always find a place to stay here that suits your wishes and needs and can serve as the perfect setting for a delightful holiday - right close to the beautiful nature and crashing North Sea.

Smoking is prohibited in all holiday accommodations and pets are not permitted in the E4 and E2 apartments.
So I can control the:
power, lights, hvac
ice skating rink, garage doors
water pressure and boilers

Of something like 36
businesses
all in one town?
What about phones?

Phones indexed by shodan!
Escape character is '^['.

OS-9/68K V3.3  Econolite 2070-1B(68360) 2002 TEES Erratum 2 - 68300  12/05/24 04:24:21

User name?:
Who?

Warning!
Shutting off controller while running
the flash memory test may corrupt files,
or other data on the flash drive.

*** DAT Main Menu ***
1) Processor
2) Front Panel
3) I/O Card
4) Async Ports
5) Sync Ports
6) Module Tests
7) Utility Functions
8) Run Continuous
9) Configure Standard Tests
AUTOPLATE.
Not red-light cameras...
something else
PIPS: The company that makes autoplate.
PIPS: want license plates?
DakTronics.
DakTronics.
Ruggedcom!
Ruggedcom!

![N4-DLC Passwords]

- **Auth Type**: Local
- **Guest Username**: guest
- **Guest Password**: guest
- **Confirm Guest Password**: guest
- **Operator Username**: operator
- **Operator Password**: operator
- **Confirm Operator Password**: operator
- **Admin Username**: admin
- **Admin Password**: admin
- **Confirm Admin Password**: admin

[Apply] [Reload]
Malware on safari?
kW? .. wat.
Dam Fumel residents want assurances

A MEETING WAS HELD YESTERDAY IN FUMEL THE FLOODS LAST FRIDAY, IN THE PRESENCE OF ALL PARTIES AND RESIDENTS.

Growing next to a dam. Delicate question which rested on Friday when the waters of the dam Fumel began to rise. Quickly. Very quickly. Too fast for riparian floats. At that point one of them even got up to 30 inches of water in his house. Some seniors even had "the fear of their lives when some electrical appliances began to crack." How to live next to a dam if you do not know what can happen.

Yesterday, a meeting was organized in Fumel in the presence of all the authorities to take stock of the situation. And very soon, it seems that the appearance of criminal acts Friday has passed. This confirmed that the building manager Philippe Gronchi for "energy Fumel": "We fully recognize our responsibility and of course we will draw the consequences. This dam is an old building which dates from 1943, bought the company in 2005 Sogatoc. We have already achieved more than 14 million euros investment and probe this issue, because it is a problem of probe will be resolved as soon as possible."

In the audience, listening but we are still angry. "Before, it never happened. There, that's three that we suffer floods in 9 years. You understand that we are tired all the more that we are not and never prevents as soon as the water rises, it is we who call the fire department. In addition, there are many older people who live in fear. We would like this to stop, said a local resident.

an alarm float

Philippe Gronchi speaks again: "We had a second warning that Sunday has confirmed that this was a concern of the probe. Of course, we will soon be remedied this problem by doubling the particular probe. In the meantime, there will be someone who will be present to manage the flow." Later, an alarm float should be installed at Condat to prevent rising waters. And the head of the DRiRE adds: "In the past, there was an agreement that was signed between EDF and the factory. At each rising waters, signaling was performed. It might be good to update this agreement." But certainly the rising water was normally regulated in recent years without automatic warning from the factory.

Another point discussed during the meeting last night, the insurance. Again, residents were reassured by the firm that provides the dam. Damage will be covered only necessary that such residents concerned make a declaration to their insurance as soon as possible, which will then return. And the mayor of Fumel, Jean-Louis Costes, also ask that the insurance can pay more quickly damaged equipment.

"Laurent Michel Lasserre with Moary"
I put that on twitter.

A day later DHS called my cellphone.
Also, that UI was built in frontpage.
YES, FRONTPAGE.
ON SCADA.
AND

SOMEONE

BOUGHT

IT
THEN PUT IT ON THE INTERNET
*ahem*
You’d think they’d LEARN.
.. but they dont.
.. they really dont.
.. they really dont.
Satellite systems
NAS storage arrays

![Synology Disk Station Manager 2.2 login screen](image-url)
“LaserWash”
Car Wash Systems
# Humidifiers

## System Status

<table>
<thead>
<tr>
<th>DEMAND</th>
<th>OUTPUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>44.9%</td>
<td>44.8%</td>
</tr>
</tbody>
</table>

**Run Mode**: Auto

**Tank Status**: Boiling

## Alarms

- 0 active alarms

## Messages

- 0 active messages

## TANK STATUS:

- **Run Mode**: Auto
- **Input Signal**: 4.5 VDC
- **Steam Output**: 44.8%
- **Steam Production**: 8 lbs/hr
- **Duct HLT Switch**: Closed
- **Tank Temperature**: 218°F
- **Tank Temp Signal**: 1745 Ohms
- **DL Low Water Switch**: Water
- **Fill Valve**: Open
- **Drain Valve**: Closed
- **Airflow Switch**: Flow
- **Interlock Switch**: Closed
- **H2O Until Service**: 1163 lbs
Humidifiers

Connect directly to the board
Emergency Telco gear

Resources
- Download PDF
- Download the Detailed Product Overview

5000S ESA Switch
Aztek Networks' 5000S ESA switch is the first and only purpose-built true emergency stand-alone switching device that is fully redundant, field cabinet ready and truly capable of seamless interoperability with any open-standard ER-303 access element or host switch.

The Aztek 5000S continuously monitors the signal between a host switch and an access device such as a DLC, BLC or MSAP, and becomes the active switching element only if the signaling link between the host switch and the access device becomes inactive.
Emergency Telco gear
wait what?

// You are free to copy the "Folder-Tree" script as long as you
// keep this copyright notice:
// Script found in: http://www.geocities.com/marcelino_martins/foldertree.html
// Author: Marcelino Alves Martins (http://www.mmartins.com)

// Log of changes:
// 10 Aug 01 - Support for Netscape 4
// 17 Feb 98 - Fix initialization flashing problem with Netscape
// 27 Jan 98 - Root folder starts open; support for GETTEXTLINKS; make the file a js file

// Definition of class Folder
.. speakers?
A massive wine cooler
A massive wine cooler
Science!
Science!
Science!
Science!
Almost all of those are offline now.

THANK YOU CERN :D
Ski trip, anyone?
Massive solar arrays
Massive solar arrays
Massive solar arrays
Massive solar arrays
Home Automation

Status: Off
Occupancy: Occupied Night
Upstairs Temp: 69.0
Upstairs Setpoint: 70 °F
Downstairs Temp: 66.6
Downstairs Setpoint: 67 °F
Garage Door: OFF
Alarm State: Disarmed

Lighting
Security
HVAC
Weather
.gov oopsies
.gov oopsies
Overview:

Tranzeo Wireless Technologies has received FCC approval on the TR-49 Series of product which is designed specifically for Homeland Security use in the 4.9 GHz frequency band. This spectrum has been allocated by the Federal Communications Commission for the exclusive use of Municipal, State and Federal Agencies.

Tranzeo Wireless Technologies products in this spectrum allow for the rapid deployment of Wireless Networks facilitating such varied uses as Video Conferencing; rapid internet and database access to vital data such as maps, building layouts, medical files and missing person images; Voice over IP (VoIP) communication; and audio/video surveillance.

These product lines represent a monumental shift in Tranzeo's product offerings, as all previous products operated on unlicensed frequencies.
.gov oopsies
... a fishery?
... a fishery?
I’m in your scadas..
Wait, no, lobster chillmode
Cant forget the champagne!
Swimming pools!
Swimming pools!

WHAT THE HELL

Thursday, April 11, 13
Swimming pools!
... really?
An acid pump?
... really?
An acid pump?
Consider the following:
so 80s style horror flick scenario

(these are actually defcon goons in a pile..)
so jason vorhees shows up...
But his victims are soup.
He’s gonna be PISSED.
So, Say you find stuff on your banjo dinosaur knitting adventure

A lot of stuff.

50,000+ results...wat do?

h/t @travisgoodspeed
Screenshot
All
THE THINGS!
:D
50k sites by hand sucks

screenshots are WAY faster! :D

Thursday, April 11, 13
I had help too

https://github.com/PaulMcMillan/eagleeye2
you can do this with vnc
Maybe you want to pwn
Pipe output to metasploit/armitage/teamsserver!
The best defense is a good offense, right?

Run this stuff on yourself. The attackers already do.
Spot outliers.

Does your staff setup EC2 instances without approval from the business? Other sites?

What else is connected to the internet, with YOUR COMPANIES NAME on it, that you don’t know about?

Who actually LIKES random, unknown liability?
Some cool new features:

You can search by:

org:
city:
country:
state:
net:
You guys are awesome
Thank you for letting me rant!

github.com/Viss/Eagleeye

github.com/PaulMcMillan/eagleeye2

Twitter: @Viss
atenlabs.com