THE RETURN OF DRAGONS
SHODAN
HTTPS://WWW.SHODAN.IO
SEARCH ENGINE OF INTERNET-CONNECTED DEVICES
GOOGLE FINDS WEBSITES

SHODAN FINDS DEVICES
The search engine for Webcams

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.
STATELESS SCANNING

C++  python™
5 Minutes
# shodan scan internet 443 https
1. Policy Impact
2. Network Security
3. Malware
4. Security Rating
5. Market Research
O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-based Netsweeper’s Role in Pakistan’s Censorship Regime

June 20, 2013

Tagged: Netsweeper, Pakistan

Categories: News and Announcements, Reports and Briefings, Research News

Download PDF

O Pakistan, We Stand on Guard for Thee:
An Analysis of Canada-based Netsweeper’s Role in Pakistan’s Censorship Regime

Summary of Key Findings

- Netsweeper filtering products have been installed on Pakistan Telecommunication Company Limited (PTCL)’s network. PTCL is Pakistan’s largest telecommunications company and also operates the Pakistan Internet Exchange Point.

- Netsweeper technology is being implemented in Pakistan on PTCL for the purposes of political and social filtering, including websites relating to human rights, sensitive religious topics, and independent media.

- In addition to using Netsweeper technology to block websites, ISPs also use other less transparent methods, such as DNS tampering.

Introduction
Total Hosts
223,260

TOP SERVICES

<table>
<thead>
<tr>
<th>Service</th>
<th>Low Occurrence</th>
<th>Medium Occurrence</th>
<th>High Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>198,659</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP S (8443)</td>
<td>23,707</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POP3 + SSL</td>
<td>284</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMAP + SSL</td>
<td>252</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SVN</td>
<td>94</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Malware
Hacked By HolaKo

DigitalOcean
Added on 2015-05-28 00:50:38 GMT
Netherlands, Amsterdam

HTTP/1.1 200 OK
Date: Thu, 28 May 2015 00:58:21 GMT
Server: Apache/2.4.6 (CentOS) mod_fcgid/2.3.9 PHP/5.5.22 Phusion
X-Powered-By: PHP/5.5.22
Content-Length: 617
Content-Type: text/html; charset=UTF-8

Hacked by Team_CC

XL Internet Services B.V.
Added on 2015-05-27 15:29 GMT
Netherlands

HTTP/1.1 200 OK
Date: Wed, 27 May 2015 22:15:13 GMT
Server: Apache/2.2.14 (Ubuntu)
X-Powered-By: PHP/5.3.2-ubuntu4.38
Vary: Accept-Encoding
Content-Length: 1426
Connection: close
Content-Type: text/html

Hacked By Lou sh

a52-181.348.138
a52-101.248-138 ltdxs4all.nl
XL Internet Services B.V.

HTTP/1.0 200 OK
Date: Sat, 23 May 2015 15:37:41 GMT
1. GHoST61: 57
2. OxFoRD & Omis Exe: 54
3. Kuroi'SH: 41
4. Oum99: 40
5. Oussama911: 37
6. Best Cracker: 35
7. root-x: 31
8. Prodigy TN: 25
9. Technical: 25
10. koat_halk_palesten: 24
Security Rating
$2 BILLION
THE INTERNET OF THINGS
MACHINE ←→ MACHINE
QUANTIFIED WORLD
Egg Minder
THE SMART EGG TRAY
why the [redacted] does my fridge need twitttr
PLEASE RATE OUR TOILET!

Excellent  Good  Satisfactory  Poor  Very Poor

Housekeeping Hotline: 91445414
This screen is sanitised regularly
Universities Needing Toner

#1 Minnesota 89
#2 Hawaii 75
#3 Austin 60
#4 San Francisco 60
#5 Toronto 56
#6 Santa Cruz 55
#7 South Florida 55
#8 Boston 55
#9 Washington 54
#10 Pennsylvania 48
NUMBER OF TURBINES
The Hyper Connected World IS NOW
1. Physical Device
2. Vendor Network
3. Maintenance
4. Privacy
Top Organizations

- Verizon Wireless
- AT&T Internet Services
- Comcast Business Communications
- CenturyLink
- Comcast Cable
- Orange
- Telefónica Internet
- Telefónica de España
- Time Warner Cable
- Vodafone Italia
NO AUTHENTICATION
Map of Industrial Control Systems on the Internet

https://icsmap.shodan.io

What is an Industrial Control System?
In a nutshell, industrial control systems (ICS) are computers that control the world around you. They’re responsible for managing the air conditioning in your office, the turbines at a power plant, the lighting at the theatre or the robots at a factory.

Learn more about ICS

Power Plants on the Internet? Really?

Why are they on the Internet?

See the Presentation
The latest research that generated the above map is being presented at the 4SICS conference in Stockholm. Visit the website to see the video once it becomes available.

4SICS Conference
DEVICE SECURITY
# telnet 192.168.1.50
Password:
Telnet is only there right now for debugging on our end and will eventually not even be compiled into the hub firmware. Kris for now Eric is right, email us at support@smartthings.com and we'll give you specific instructions on how to remove a z-wave device. Right now when you remove a z-wave device, the hub goes into "zwave exclude mode" for 10 seconds, and we are working on adding a z-wave remove button in the mobile app.
Quirky needs your Wink Hub back after a botched security update

After a failed security update, Quirky asks Wink Hub owners to send their units in for a repair.

by Rich Brown / @rh_brown / April 19, 2015 6:01 AM PDT
VENDOR NETWORK
Cluster: elasticsearch
Number of nodes: 2
Status: yellow

Experimental cluster Pack diagram:
OpenDNS
3 Memcache
13 VNC
38 Telnet
1 Heartbleed
9 FREAK

34% of Vendors
MAINTENANCE & OPERATION
Fridge sends spam emails as attack hits smart gadgets

A fridge has been discovered sending out spam after a web attack managed to compromise smart gadgets.

The fridge was one of more than 100,000 devices used to take part in the spam campaign.

Uncovered by security firm Proofpoint, the attack compromised computers, home routers, media PCs and smart TV sets.

The attack is believed to be one of the first to exploit the lax security on devices that are part of the "Internet of things".

The fridge was one of 100,000 devices used as part of the spam attack.

The fridge was one of more than 100,000 devices used to take part in the spam campaign.

Uncovered by security firm Proofpoint, the attack compromised computers, home routers, media PCs and smart TV sets.

The attack is believed to be one of the first to exploit the lax security on devices that are part of the "Internet of things".

The spam attack took place between 23 December 2013 and 6 January this year, said Proofpoint in a statement in total, it said, about 750,000 messages were sent as part of the junk mail campaign. The emails were routed through the compromised gadgets.

Related Stories

Connected tech sparks privacy fears
LG promises fix for "spying" TVs
Food byte: The kitchen goes digital

Top stories

Israel calls up 16,000 reservists
Leaders meet to discuss MH17 access
Race to find India landslide missing
Argentina defaults for second time
Liberia shuts schools over Ebola

Features & Analysis

Tiki taste
Why the Tiki bar became an American phenomenon
Black trailblazer
US Vogue's first African American cover girl 40 years on
Mystery woman
The figure clad in black, walking across the US
Information spread
Just what are the dangers of the Stuxnet effect?

Most Popular

Israel calls up 16,000 reservists
House votes to sue President Obama
Nato "unprepared for Russia threat"
PARIS — France is ordering manufacturers to inform consumers how long they can expect their TV, cell phone or other appliance to last — before they buy it.

A new French government decree that came into effect this week aims at fighting so-called planned obsolescence. That is when companies design strategies to limit the life span of appliances, so that consumers will have to replace them.

The measure requires manufacturers to inform vendors how long spare parts for an appliance will continue to be produced. The vendor is then required to inform the buyer, in writing. Violators face up to 15,000 euros ($16,800) in fines.

A similar French measure coming into effect next year will require manufacturers to replace or repair faulty appliances for free for the first two years after purchase.
CCTV cameras secretly being switched off by cash-strapped councils
PRIVACY IMPLICATIONS
iOS 7
iBeacons
EXAMPLE: LICENSE PLATES
This web interface will help you understand the system. Ideally, you should have a copy of the manual. This explains what the values mean.

Online Help is available for every field and the bottom of screen.

If you have any comments or questions, please feel free to contact us. The telephone number is [redacted]. Thanks!

[Images of car license plates and data transfer windows]

Display Type: [Any camera] Data transfer: Stop

Gain/Shutter: 2/11 Plate: VOB939 Width: 720 Confidence: 86:1824

Gain/Shutter: 2/9 Plate: DBGF177 Width: 720 Confidence: 81:1773

Gain/Shutter: 2/11 Plate: X289102 Width: 720 Confidence: 84:1853

[Data transfer output shown in the image]
100 Cameras
5 Days
62,857 Unique License Plates
SEWTHIS
EMBALMR
CUISINE
GOODDAY
1.3% Novelty Plates
National Vehicle Location Service (NVLS)

The National Vehicle Location Service (NVLS) is a national data sharing initiative started by Vigilant in 2008. The data in NVLS is made up from two primary sources: 1) data shared to Vigilant by law enforcement agencies and 2) data from the National Vehicle Identification System (VIN) database.

System Specifications
- Secure and hosted LPR data for law enforcement only
- Private LPR data collection of over 70 million records per month
- Accessible via an Agency’s LEARN account
- Hotlist matching and alerting capabilities

System Application & Benefits
- Improved investigative data set
- Locate vehicles of interest
- Increase investigative leads

Technical Datasheets NVLS
- LEARN Datasheet
- LPR Data (NVLS) Datasheet
Our Goals for the "Internet of Things"

- **FOCUS** effort towards crowd-funded, small commercial and bootstrapped vendors
- **BUILD** partnerships and goodwill between IoT vendors and the security community
- **COORDINATE** efforts to incentivize security researchers for reporting vulnerabilities
- **CURATE** informational resources to help educate vendors on security best practices
- **PRESENT** research at relevant events and be a point of contact for press inquiries

Vendors Participating With BuildItSecure.ly

**pinoccio**

Pinoccio is a complete toolkit for building the Internet of Things. Makers, Software Developers, and Product Designers can use the tiny microcontroller to quickly prototype ideas. It has mesh networking and wireless web connectivity baked right in. Pair that with the REST API and web app, and you have an end-to-end system that works right out of the box.

**dropcam**

Dropcam is a cloud-based video monitoring service with free live HD streaming, two-way talk and mobile apps that makes it easy to stay connected to places, people and pets, no matter where you are. Featuring automatic updates, stream sharing, location awareness and optional Cloud Recording, Dropcam has redefined home monitoring and do-it-yourself security.

**zendo**

Zendo is a South Florida-based technology company that creates, designs, and manufactures simple devices for custom home monitoring and control, as well as best-in-class apps and services. Zendo products will be available at leading retailers.

**DipJar**

DipJar is the first-ever tip jar and donation box for credit and debit cards, a hardware/software solution for one-step collection and seamless disbursement of electronic donations.
Internet of Things Nmap Fingerprints

A repository of Nmap scans for various IoT devices. The following command was run to perform the scan:

```
nmap -Pn -p -A -oX <name> <ip>
```

Where `name` is a descriptive name for the device (ex: "wink-hub") and `ip` is the IP address the device has on your local network.

To have your Nmap scan results added to this repository either submit a pull request or send your XML file to support@shodan.io

[github.com/shodan-labs/iotdb](https://github.com/shodan-labs/iotdb)
Questions?