

Cyber Threats

November, 2015



Background



- 2010-2012 - WikiLeaks released information Iraq War, Afghan War, Guantanamo Bay, Diplomatic Cables, Stratfor, etc.
- 2011 – Anonymous Group LulzSec and AntiSec begin to expand targets to include Government (CIA, FBI, Congress, Etc)
- 2011-2012 - Occupy Wall Street followed by numerous protests in other cities across the nation.
- 2011-2012 - Articles are published announcing the NSA Data Storage facility in Lehi, Utah.

Utah Events



- January 2012 - “Cabin Crew” targets Utah
 - Utah Chiefs of Police Association website hacked
 - Salt Lake City Police Department website hacked
- March 2012 – Health Breach

Current Threats



- Activists - Extremists
- Criminal
 - Single Actor
 - Teams / Groups
 - Commercial / Organizations
- State Sponsored
- Terror Related

Activists - Extremists



- Ferguson
- Darrien Hunt
- Environmental Groups
- Vikingdom
- LulzSaints
- TeamPoison

Communication Methods



- Twitter
- Facebook
- Pastebin
- Dark Web Forums
- YouTube
- Chat Rooms

Common Activities



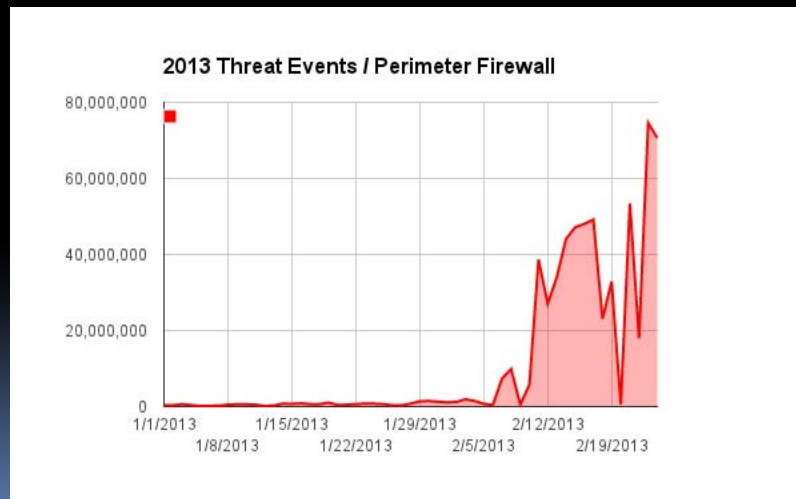
- Denial Of Service (DOS)
- “Doxing” Posting of Personal Information
- Socially Engineered Attacks
- Defacements - Hacks – SQL Injection - Dumps
- “SWATing”
- Extortion - Crypto Locker

Common Activities - Continued

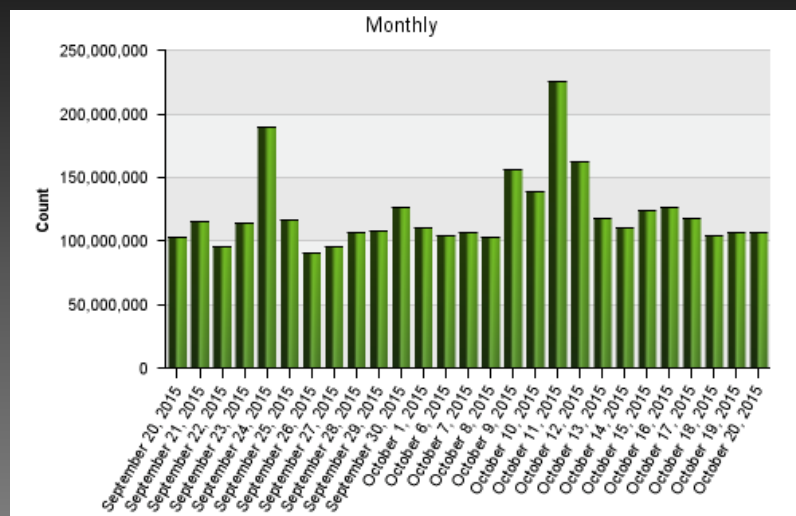


- Email Attacks – Malware – Loaders – Redirectors
- Mobile Device Attacks
- Trolling – Cyber Bullying
- Black Faxing
- Protest Organization

Blocking Profile Jan-Feb 2013



Blocking Profile Sept – Oct 2015



DDOS



Pinned Tweet
Vikindom2015 @Vikindom2015 · 10h
 Warning to America
soundcloud.com/vikindom2015-...
 [REDACTED]
 [REDACTED]
 US Target List
pastebin.com/4FtKhSRN
 [REDACTED]
 SoundCloud

DDOS – Reverse Logging



Pinned Tweet
Vikindom2015 @Vikindom2015 · 59m
 YoU gOt HaCkEd Maine
 ALL IP ADDRESSES LOGGED
 MASSIVE LIST
pastebin.com/xvrfPGZf

25.03.2015 13:36:43	96.221.179.20	United States	Maine
25.03.2015 15:56:32	66.231.195.50	United States	Maine
25.03.2015 15:56:19	74.113.160.154	United States	New York
25.03.2015 15:55:34	173.209.211.145	United States	California
25.03.2015 15:54:32	198.255.176.91		
25.03.2015 15:54:03	86.174.112.76	United Kingdom	London, City of
25.03.2015 15:53:05	76.174.112.76	United States	New Hampshire
25.03.2015 15:52:56	70.192.17.89	United States	
25.03.2015 15:52:39	216.220.227.131	United States	Maine
25.03.2015 15:50:44	66.231.195.50	United States	Maine
25.03.2015 15:50:03	66.231.195.50	United States	Maine
25.03.2015 15:48:48	76.179.86.149	United States	Maine
25.03.2015 15:48:45	199.38.154.10	United States	Illinois
25.03.2015 15:48:24	54.163.32.75	United States	New Jersey
25.03.2015 15:47:54	64.223.170.121	United States	Maine
25.03.2015 15:46:53	87.183.129.16	Germany	Nordrhein-Westfalen
25.03.2015 15:46:14	67.253.23.66	United States	Maine

View more photos and videos

Vulnerability Intercept



TeaMp0isoN @_TeaMp0isoN · 12h

Utah Department of Health - SQLi Vulnerable
(scroll down) - #TeaMp0isoN

health.utah.gov/myhealthcare/r...

3 3 ...

Logging after Post



35	3/18/2015 21:21:43	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	FR	37.187.129.166	59695	US	168.180.174.106
36	3/18/2015 21:20:43	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	FR	37.187.129.166	51928	US	168.180.174.106
37	3/18/2015 21:19:43	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	FR	37.187.129.166	58221	US	168.180.174.106
38	3/18/2015 21:18:53	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	DE	85.25.103.119	53288	US	168.180.174.106
39	3/18/2015 21:17:47	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	FR	37.187.129.166	58970	US	168.180.174.106
40	3/18/2015 21:16:48	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	US	96.47.228.22	41275	US	168.180.174.106
41	3/18/2015 21:15:54	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	RO	109.163.234.4	60415	US	168.180.174.106
42	3/18/2015 21:13:44	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	DE	85.25.103.119	43979	US	168.180.174.106
43	3/18/2015 21:12:42	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	RO	109.163.234.4	4996	US	168.180.174.106
44	3/18/2015 21:11:44	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	DE	85.25.103.119	43975	US	168.180.174.106
45	3/18/2015 21:10:42	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	FR	37.187.129.166	51994	US	168.180.174.106
46	3/18/2015 21:09:43	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	RO	109.163.234.4	42376	US	168.180.174.106
47	3/18/2015 21:08:43	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	FR	37.187.129.166	57699	US	168.180.174.106
48	3/18/2015 21:08:16	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	DE	85.25.103.119	53714	US	168.180.174.106
49	3/18/2015 21:06:43	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	FR	37.187.129.166	40952	US	168.180.174.106
50	3/18/2015 21:05:43	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	DK	82.211.223.3	33708	US	168.180.174.106
51	3/18/2015 21:04:43	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	FR	37.187.129.166	42696	US	168.180.174.106
52	3/18/2015 21:03:43	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	FR	37.187.129.166	36797	US	168.180.174.106
53	3/18/2015 21:02:42	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	DK	82.211.223.3	36901	US	168.180.174.106
54	3/18/2015 21:01:53	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	RO	176.126.252.11	60618	US	168.180.174.106
55	3/18/2015 21:00:54	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	US	96.47.228.22	36306	US	168.180.174.106
56	3/18/2015 20:59:44	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	DE	85.25.103.119	42547	US	168.180.174.106
57	3/18/2015 20:58:44	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	RO	176.126.252.11	36586	US	168.180.174.106
58	3/18/2015 20:57:43	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	RO	176.126.252.11	58186	US	168.180.174.106
59	3/18/2015 20:56:43	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	DE	85.25.103.119	46925	US	168.180.174.106
60	3/18/2015 20:54:42	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	DK	82.211.223.3	54414	US	168.180.174.106
61	3/18/2015 20:53:42	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	DE	85.25.103.119	49470	US	168.180.174.106
62	3/18/2015 20:50:42	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	RO	176.126.252.11	13292	US	168.180.174.106
63	3/18/2015 20:49:53	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	DK	82.211.223.3	53114	US	168.180.174.106
64	3/18/2015 20:48:45	HTTP SQL Injection Attempt(30514)	drop-all-packets	medium	1	FR	37.187.129.166	39182	US	168.180.174.106
65	3/18/2015 20:47:38	HTTP SQL Injection Attempt(30338)	drop-all-packets	medium	1	FR	37.187.129.166	56234	US	168.180.174.106
66	3/18/2015 20:45:23	HTTP SQL Injection Attempt(30338)	drop-all-packets	medium	1	US	96.47.228.22	51315	US	168.180.174.106

Criminal – Commercial Hacking



HackPal.com

Submit your email hacking order

ENTER TARGET EMAIL ADDRESS [HACK IT NOW](#)

\$150.00

EMAIL PASSWORD HACKING

When you have the feeling that you are created by your wife/husband / maybe friend/friend an email hacking service is the only way to know the truth. We have almost 10 years of experience in online surveillance & password recovery. Our service is intended to permit our customers to verify the integrity of their interpersonal relationships and to ensure the safety and well-being of their family.

[LEARN MORE](#) [ORDER NOW](#)

[How much does it cost?](#) [How it works](#) [About us](#)

Yahoo Password	Gmail Password	Hotmail Password	Private Email Hacking	Facebook Password
\$150.00 per password	\$150.00 per password	\$150.00 per password	\$350.00 per password	\$300.00 per password
ORDER NOW	ORDER NOW	ORDER NOW	ORDER NOW	ORDER NOW
Provides original password No security alert generated Rogers, ATT & SBCglobal Also include Ymail Hacked within 72 hrs	Provides original password No security alert generated Include Gogmail The password is not reset Hacked within 72 hrs	Provides original password Works for Outlook.com No security alert generated MSN, Windows and Live Hacked within 72 hrs	Provides original password Provides login link Explains how to log in The password is not changed Hacked within 1 week	Provides original password Bypass security checks No security alert generated The password is not changed Hacked within 1 week

Criminal – Credit Card Sales



EVEN MORE USA DUMPS UPDATED / 07 SEPTEMBER 2014 / COMMENTS:

Even more USA Dumps updated!

Base name: **American Sanctions 6, 7, 8, 9**
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

Base name: **American Sanctions 10, 11, 12**
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

USA DUMPS UPDATE! / 04 SEPTEMBER 2014 / COMMENTS:

USA Dumps update you asked for!

Base name: **American Sanctions 5**
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

Base name: **American Sanctions 4**
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

Base name: **American Sanctions 3**
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

Criminal – Commercial Scanning



Shodan Exploits Scanhub Maps Blog Anniversary Promotion Register Login

SHODAN Search

EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

[TAKE A TOUR](#) [FREE SIGN UP](#)

Popular Search Queries: IOmega NAS Devices (no passwords) - A bunch of external hard drives without passwords attached to the Interbuttz

**DEVELOPER API**
Find out how to access the Shodan database with Python, Perl or Ruby.

**LEARN MORE**
Get more out of your searches and find the information you need.

**FOLLOW ME**
Contact me and stay up to date with the latest features of Shodan.

Scanning Results



Criminal – Commercial



Shodan Exploits Scanhub Maps Blog Anniversary Promotion Settings Logout Buy ?

SHODAN Search

Home Search Directory Data Analytics/ Exports Developer Center Labs

Popular Searches Recently Added Browse Tags

Browse All Searches

Tag: camera

30 OCT 12 **Red light enforcement cameras** 64
red light enforcement camera webcam
red light enforcement camera webcam

30 APR 13 **D-Link Internet Camera** 60
D-Link Internet Camera DCS-5300 series, without authentication. [google 5c0u7]
dlink dcs5300 webcam camera netcam no authentication

31 MAR 13 **webcamxp** 30
one of the best dorks for ip cameras/webcams
webcam cam camera ipcam ipcamera live

26 JUL 12 **yawcam** 21
yet another webcam
ip camera

25 NOV 13 **Red Light Cameras** 19
PIPS Technology ALPR processors are complete one-box processors for automatic licence plate recognition. To see a live feed of license plates as they're being captured, visit the "Monitor > Client Monitor" section.
camera http traffilight

Search the Directory

List All Searches By

» Popularity

» Recently Added

Popular Tags

webcam	60
scada	48
http	41
camera	40
router	40
ftp	36
test	35
cam	35
cisco	30
ssh	28

Criminal – Commercial



Default Password List

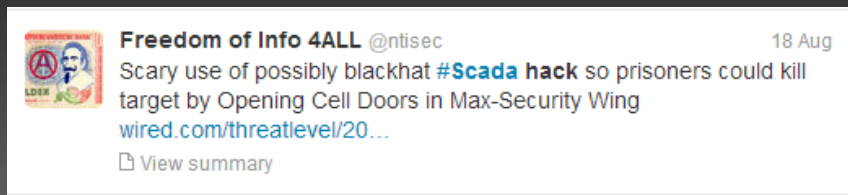
2007-07-03

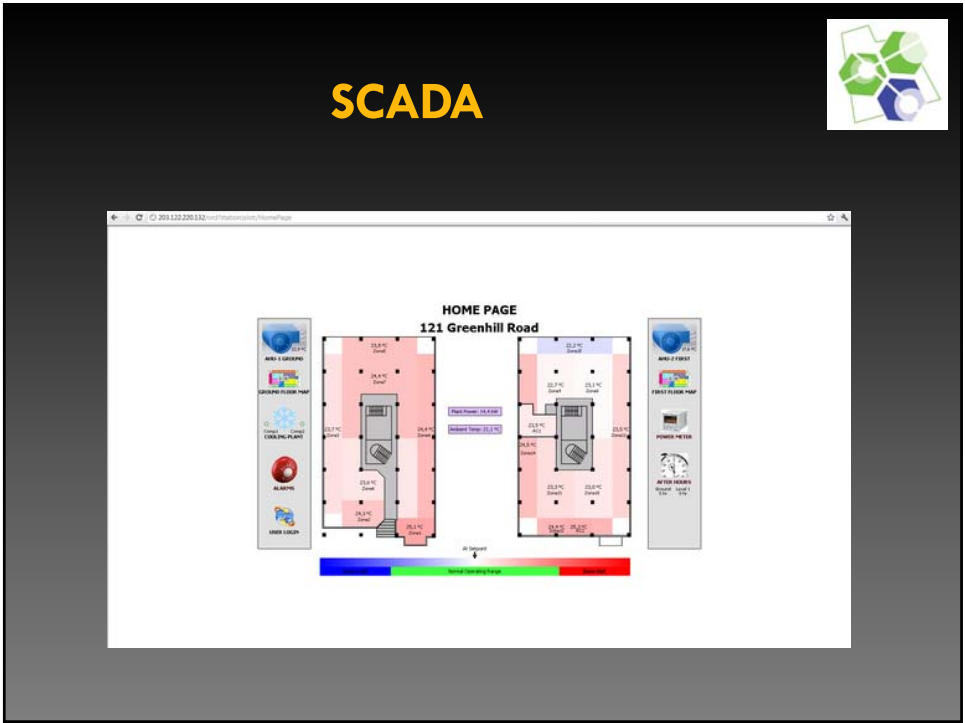
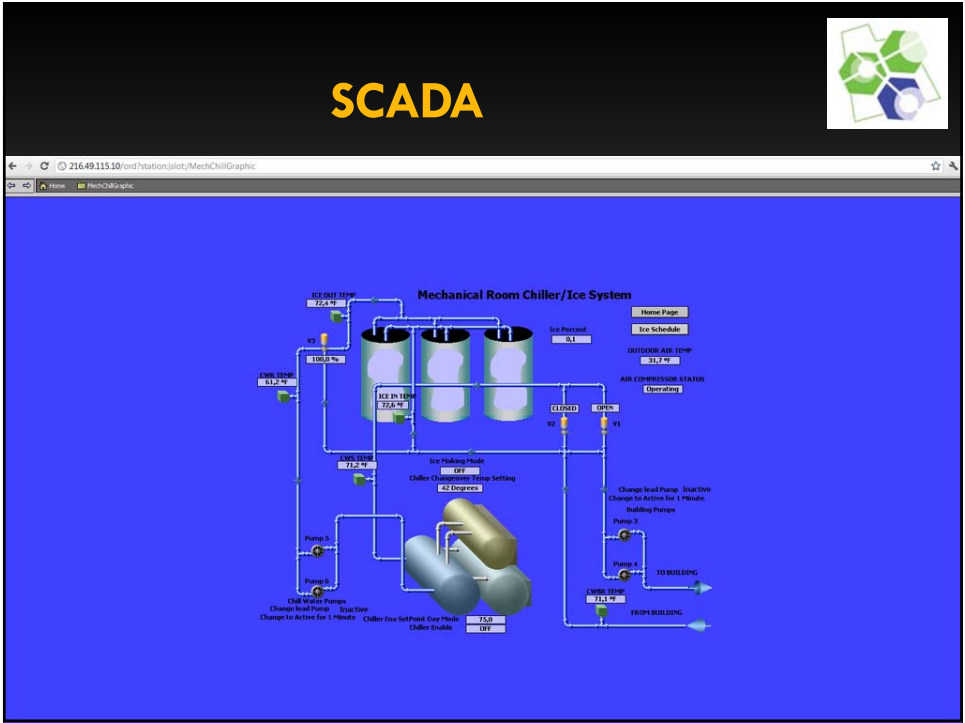
Vendor	Model	Version	Access Type	Username	PASSWORD	Privileges	Notes
ICOM	CoreBuilder	7000/6000/1500/2500	Telnet	debug	synnet		
ICOM	CoreBuilder	7000/6000/1500/2500	Telnet	tech	tech		
ICOM	HiPerARC	v4.1.x	Telnet	adm	(none)		
ICOM	LANplex		2500 Telnet	debug	synnet		
ICOM	LANplex		2500 Telnet	tech	tech		
ICOM	LinkSwitch	2000/2700	Telnet	tech	tech		
ICOM	NetBuilder		SNMP		ANYCOM	ump-read	
ICOM	NetBuilder		SNMP		ILMI	ump-read	
ICOM	NetBuilder		Mobi	admin	(none)	Admin	
ICOM	Office Connect ISDN Routers	3x0	Telnet	n/a	PASSWORD	Admin	
ICOM	SuperStack II Switch		2200 Telnet	debug	synnet		
ICOM	SuperStack II Switch		2700 Telnet	tech	tech		
ICOM	OfficeConnect 812 ADSL		Mobi	adminintl	adminintl	Admin	
ICOM	Wireless AP	ANY	Mobi	admin	comconcom	Admin	Works on all Icom wireless APs
ICOM	CdPlex		7000 Telnet	tech	tech	User	
ICOM	cdplex		7000 Telnet	admin	admin	Admin	
Icom	cdplex		7000 Telnet	operator	(none)	Admin	
ICOM	HiPerARC	v4.1.x	Telnet	adm	(none)	Admin	

SCADA



SCADA





Risk Reduction



- Policies
- Current Anti-Virus
- Education and Awareness
- Passwords – Dual Factor
- Social Media Awareness
- Personal Information Protection

Resources



- FISMA, PCI, HIPA, CJIS
- IC3.gov (FBI)
- MSISAC
- Utah Cyber Task Force

Cyber Task Force



Questions

