An Overview of ICANN's Training Program for *Investigating DNS Abuse/Misuse*

Dave Piscitello
VP, Security and ICT Coordination
John L. Crain
Chief Identifier Systems SSR Officer

Identifier Systems SSR Training Portfolio

- Registry (TLD) Operations
- Secure Registry Operations (SROC)
- DNSSEC (Robust & Reliable DNS Operations)
- Investigating DNS Abuse & Misuse
- Security Awareness for ICT end users
- Foundational Security for ICT administrators

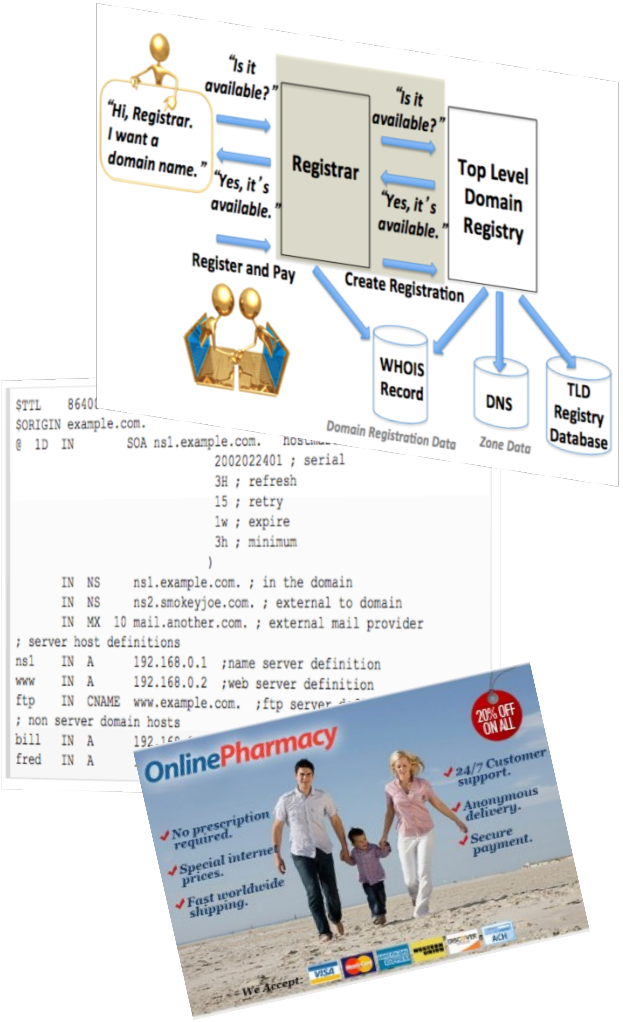
Training partners or ICANN staff
ICANN staff
Future training for trust-based collaboration partners

What We'll Discuss today

- Purpose of "Investigating DNS…"
- Topics we cover
- Who participates?
- Investigative methodology
- Resources we share

Purpose of the training

- To assist participants in understanding
  - DNS and name registration system operations
  - DNS and registration ecosystems and players
  - How criminals abuse or misuse domain names or DNS
  - How to collect indicators or evidence of abuse or misuse
  - How the data collected may be relevant to investigations



```
$TTL    8640
$ORIGIN example.com.
@  1D  IN        SOA ns1.example.com.   hostma
                              2002022401 ; serial
                              3H ; refresh
                              15 ; retry
                              1w ; expire
                              3h ; minimum
                             )
       IN  NS     ns1.example.com. ; in the domain
       IN  NS     ns2.smokeyjoe.com. ; external to domain
       IN  MX  10 mail.another.com. ; external mail provider
; server host definitions
ns1    IN  A      192.168.0.1  ;name server definition
www    IN  A      192.168.0.2  ;web server definition
ftp    IN  CNAME  www.example.com.  ;ftp server
; non server domain hosts
bill   IN  A      192.16
fred   IN  A
```

Topics we cover

- What are indicators of misuse/abuse in
  - DNS (zone) data?
  - Domain registration data?
  - DNS traffic?
  - Authoritative name servers and resolvers?
  - Addressing and routing information
- What additional information can you use?
  - Reputation (scoring) systems
  - Content analysis

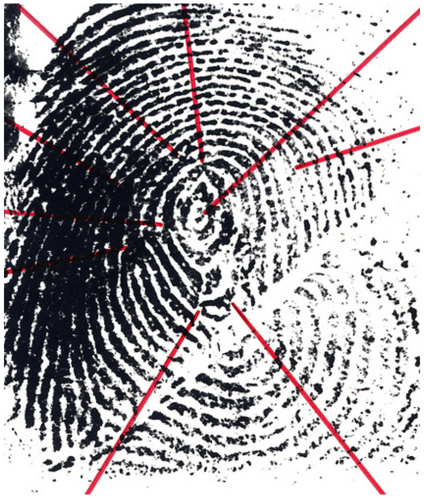
Where can you find these indicators?

- *Primary sources are publicly available*
  - The DNS
  - Domain and IP Whois
  - Web-based services
    - commercial, free, open source, research projects
- Trust-based collaborative communities
  - Interveners, researchers, investigators, operators
  - Certain of these are vetted communities

Investigative Philosophy

"Match fingerprints" analog

no one marker is sufficient to conclude a domain is malicious



Course adapts to changes in adversary behavior

Markers include checks like these…

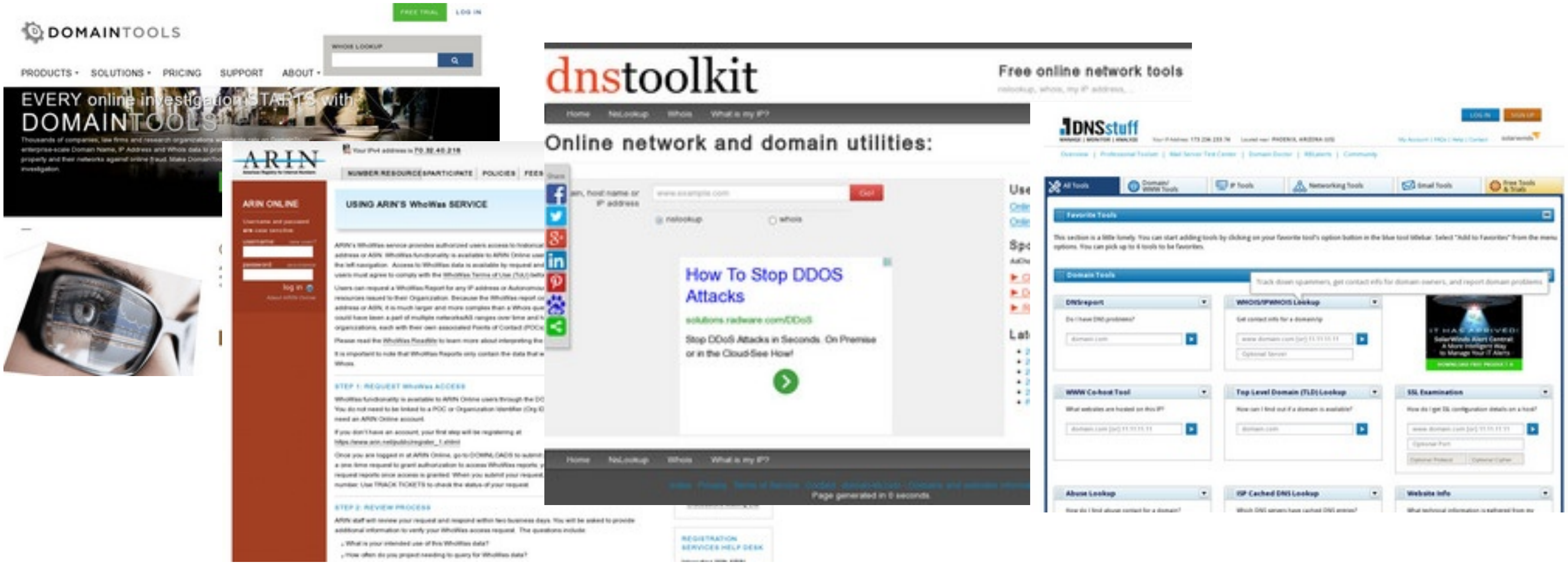
- Recent domain registration creation date
- Suspicious registrant contact data
- Privacy protection service
- Spoofing or confusing use of a brand
- Name composition or length
- Known DGA or malware control point
- High frequency/volume of Name errors
- Suspicious or notorious name servers
- Suspicious or notorious hosting location
- What's the neighborhood like?
- Base site content is non-existent or bad
- Anomalies or clues in DNS Zone data
- Reputation

Who participates?

- Individuals with roles in combatting cybercrime
  - Law enforcement
  - Jurists
  - ICT network operators (government, infrastructure, registry)
- Individuals with roles in capability building programs
  - Security community members
  - Partners in capability building collaboratives

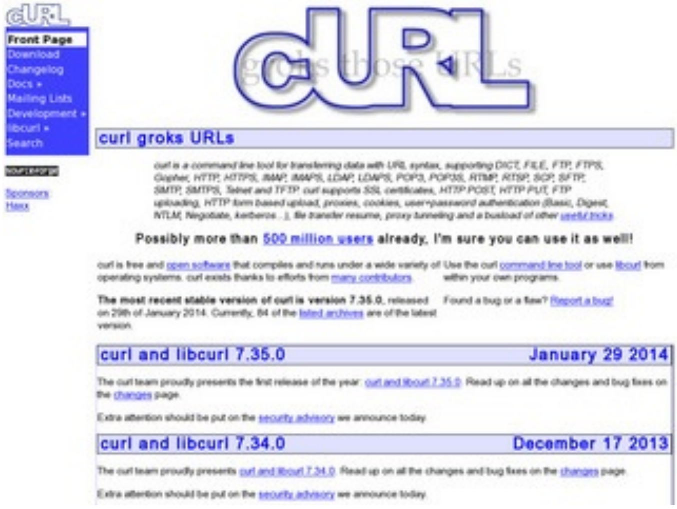
Resources We Show and Share

- Tools to identify abuse points of contact
  - Domain names, host names, IP addresses, ASNs
  - Domain and IP registrants, registries, registrars
  - DNS, Content hosting, or Mail Exchange providers



Resources we show and share

- Publicly available tools to identify, collect or analyze
  - Content (web pages, sites,
  - Malicious content (URL, file, email, attachment)
  - Reputation system operators



curl groks URLs

curl is a command line tool for transferring data with URL syntax, supporting DICT, FILE, FTP, FTPS, Gopher, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMTP, SMTPS, Telnet and TFTP. curl supports SSL certificates, HTTP POST, HTTP PUT, FTP uploading, HTTP form based upload, proxies, cookies, user+password authentication (Basic, Digest, NTLM, Negotiate, kerberos...), file transfer resume, proxy tunneling and a busload of other useful tricks

Possibly more than 500 million users already, I'm sure you can use it as well!

curl is free and open software that compiles and runs under a wide variety of operating systems. curl exists thanks to efforts from many contributors.

Use the curl command line tool or use libcurl from within your own programs.

The most recent stable version of curl is version 7.35.0, released on 29th of January 2014. Currently, 84 of the listed archives are of the latest version.

Found a bug or a flaw? Report a bug!

curl and libcurl 7.35.0 — **January 29 2014**

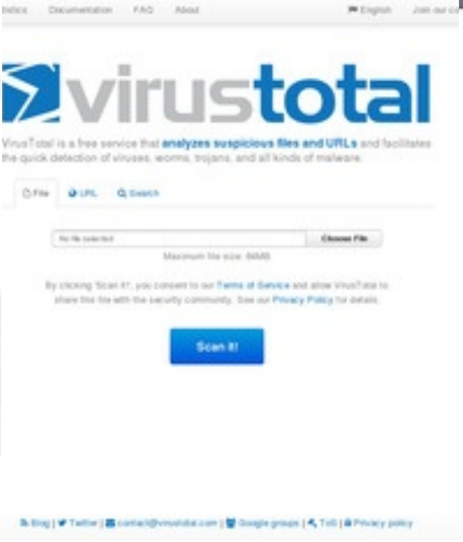
The curl team proudly presents the first release of the year: curl and libcurl 7.35.0. Read up on all the changes and bug fixes on the changes page.

Extra attention should be put on the security advisory we announce today.

curl and libcurl 7.34.0 — **December 17 2013**

The curl team proudly presents curl and libcurl 7.34.0. Read up on all the changes and bug fixes on the changes page.

Extra attention should be put on the security advisory we announce today.



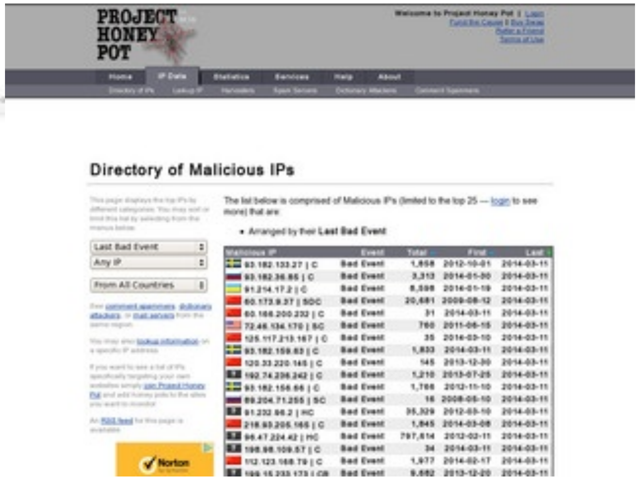
VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

No file selected

Maximum file size: 64MB

By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.

Blog | Twitter | contact@virustotal.com | Google groups | ToS | Privacy policy



Directory of Malicious IPs

This page displays the top IPs in different categories. You may sort or limit this list by selecting from the menus below.

Last Bad Event

Any IP

From All Countries

See comment spammers, dictionary attackers, or mail servers from the same region.

You may also lookup information on a specific IP address.

If you want to see a list of IPs specifically targeting your own websites simply join Project Honey Pot and add honey pots to the sites you want to monitor.

An RSS feed for this page is available.

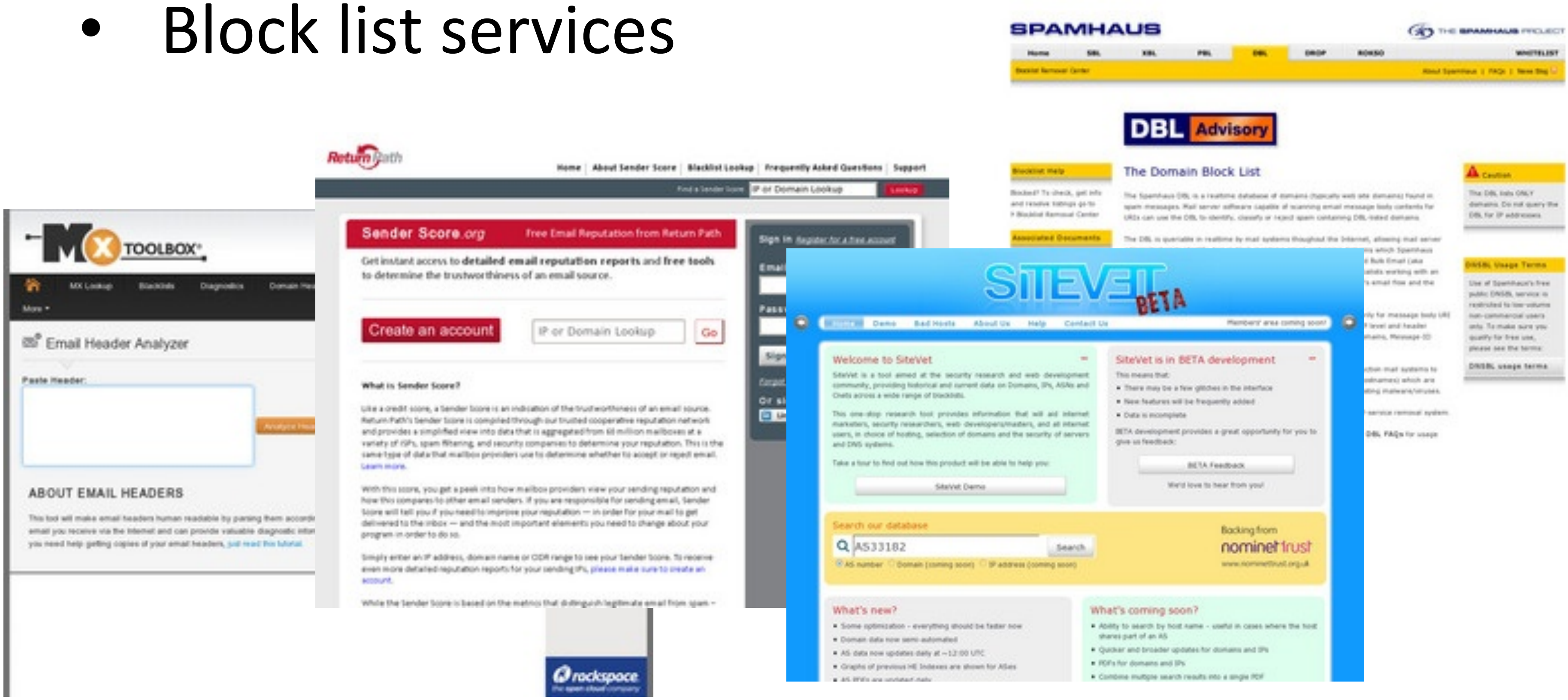
The list below is comprised of Malicious IPs (limited to the top 25 — login to see more) that are:

- Arranged by their **Last Bad Event**

Malicious IP	Event	Total	First	Last
93.182.133.27 | C	Bad Event	1,858	2012-10-01	2014-03-11
93.182.36.85 | C	Bad Event	3,313	2014-01-30	2014-03-11
91.214.17.2 | C	Bad Event	8,598	2014-01-19	2014-03-11
60.173.9.37 | SDC	Bad Event	20,681	2009-08-12	2014-03-11
60.166.200.232 | C	Bad Event	31	2014-03-11	2014-03-11
72.46.134.170 | SC	Bad Event	760	2011-06-15	2014-03-11
125.117.213.167 | C	Bad Event	35	2014-03-10	2014-03-11
93.182.159.83 | C	Bad Event	1,833	2014-03-11	2014-03-11
120.33.220.145 | C	Bad Event	145	2013-12-30	2014-03-11
192.74.236.242 | C	Bad Event	1,210	2013-07-25	2014-03-11
93.182.156.66 | C	Bad Event	1,766	2012-11-10	2014-03-11
89.204.71.255 | SC	Bad Event	16	2008-05-10	2014-03-11
91.232.96.2 | HC	Bad Event	35,329	2012-03-10	2014-03-11
218.93.205.165 | C	Bad Event	1,845	2014-03-08	2014-03-11
96.47.224.42 | HC	Bad Event	797,614	2012-02-11	2014-03-11
198.98.109.57 | C	Bad Event	34	2014-03-11	2014-03-11
112.123.168.79 | C	Bad Event	1,977	2014-02-17	2014-03-11
199.15.233.173 | CB	Bad Event	9,882	2013-12-20	2014-03-11

Tools we show and share

- Hosting (web, DNS, mail) or traffic origins
- ISPs, mail exchange, or DNS operators
- Block list services



ABOUT EMAIL HEADERS

This tool will make email headers human readable by parsing them accord… email you receive via the Internet and can provide valuable diagnostic infor… you need help getting copies of your email headers, just read this tutorial.

Get instant access to **detailed email reputation reports** and **free tools** to determine the trustworthiness of an email source.

What is Sender Score?

Like a credit score, a Sender Score is an indication of the trustworthiness of an email source. Return Path's Sender Score is compiled through our trusted cooperative reputation network and provides a simplified view into data that is aggregated from 60 million mailboxes at a variety of ISPs, spam filtering, and security companies to determine your reputation. This is the same type of data that mailbox providers use to determine whether to accept or reject email. Learn more.

With this score, you get a peek into how mailbox providers view your sending reputation and how this compares to other email senders. If you are responsible for sending email, Sender Score will tell you if you need to improve your reputation — in order for your mail to get delivered to the inbox — and the most important elements you need to change about your program in order to do so.

Simply enter an IP address, domain name or CIDR range to see your Sender Score. To receive even more detailed reputation reports for your sending IPs, please make sure to create an account.

While the Sender Score is based on the metrics that distinguish legitimate email from spam –

The Domain Block List

The Spamhaus DBL is a realtime database of domains (typically web site domains) found in spam messages. Mail server software capable of scanning email message body contents for URIs can use the DBL to identify, classify or reject spam containing DBL-listed domains.

The DBL is queriable in realtime by mail systems thoughout the Internet, allowing mail server

Blocked? To check, get info and resolve listings go to > Blocklist Removal Center

The DBL lists ONLY domains. Do not query the DBL for IP addresses.

Use of Spamhaus's free public DNSBL service is restricted to low-volume non-commercial users only. To make sure you qualify for free use, please see the terms:

Welcome to SiteVet

SiteVet is a tool aimed at the security research and web development community, providing historical and current data on Domains, IPs, ASNs and Cnets across a wide range of blacklists.

This one-stop research tool provides information that will aid internet marketers, security researchers, web developers/masters, and all internet users, in choice of hosting, selection of domains and the security of servers and DNS systems.

Take a tour to find out how this product will be able to help you:

SiteVet is in BETA development

This means that:

- There may be a few glitches in the interface
- New features will be frequently added
- Data is incomplete

BETA development provides a great opportunity for you to give us feedback:

We'd love to hear from you!

Search our database

AS33182

● AS number ○ Domain (coming soon) ○ IP address (coming soon)

What's new?

- Some optimization - everything should be faster now
- Domain data now semi-automated
- AS data now updates daily at ~12:00 UTC
- Graphs of previous HE Indexes are shown for ASes
- AS PDFs are updated daily

What's coming soon?

- Ability to search by host name - useful in cases where the host shares part of an AS
- Quicker and broader updates for domains and IPs
- PDFs for domains and IPs
- Combine multiple search results into a single PDF

Questions?