

DNS Abuse & Criminal use of the DNS

*Issues, detection, mitigation and
tools for the investigator*

*Dave Piscitello
Carlos Alvarez
Champika Wijayatunga*

Syllabus

- Brief Overview of Internet Identifiers
- Brief Overview of DNS
- Common Uses for Criminal Domains
- Domain Seizures
- Tools for Investigating Badness
(Examples, hands-on, walk-thrus)



Brief Overview of Internet Identifiers

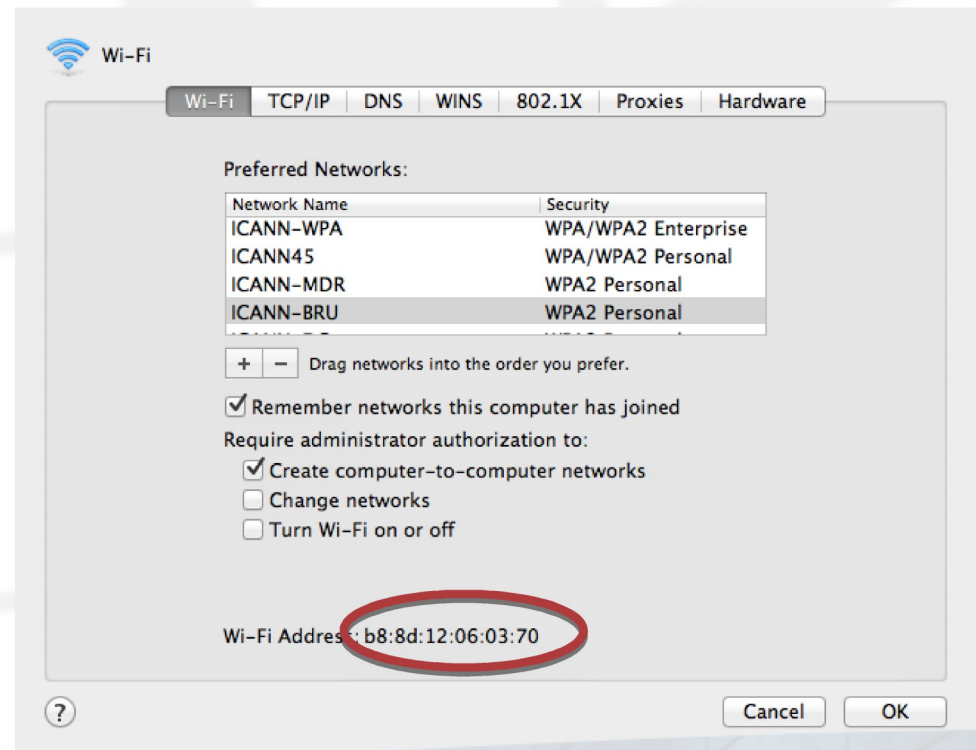
Connecting to a local network

- Every device that can connect to a local area network has 1+ hardware (MAC) address

MAC addresses are 48 bit unique identifiers

One is assigned to each network adapter at time of manufacture

Absent tampering, they do not change from network to network



Find Your MAC address

Operating System	Method
Windows Devices	Open cmd.exe, type <i>getmac</i>
Open BSD on Mac OS X and Linux	Launch Terminal, type <i>ifconfig</i> look for “ether xx:xx:xx:xx:xx”
iPhone	Settings -> General -> About then scroll to <i>WiFi Address</i>
Android	Settings -> About Tablet -> Status then scroll to <i>Wi-Fi MAC address</i>

How to connect to an IP network

- Every device that connects to an *IP* network must have an Internet Protocol (IP) address
- Two classes of IP addresses
 - Class A or IP version 4 addresses are typically represented as *dotted decimal numbers*, e.g.
192.168.2.1
 - Class AAAA or IP version 6 addresses are ugly hexadecimal things with “:” as separators, e.g.,
fe80::226:bbff:fe11:5b32

Connecting to the Internet

- Your device also needs to know how to reach destinations beyond your local network
 - A *gateway* can provide this information using *DHCP*
- Your device relies on this gateway to route IP traffic to and from Internet destinations



Can someone help
me join a network?



Welcome! I'm your gateway

- My address is 192.168.4.1
- Your IP address is 192.168.4.94
- Your subnet is 255.255.252.0

Associating MAC and IP addresses

- MAC addresses are “hard-wired” *but* user devices typically obtain local network IP addresses dynamically
- Your device can communicate directly with other devices and servers on your local network
 - Devices use the *Address Resolution Protocol* to see MAC and IP addresses on your local network

Use this
command
to see
your ARP
table

```
dave — bash — 68x10
login: Thu May 22 11:34:52 on ttys000
dave$ arp -a
? (172.17.1.1) at c0:ea:e4:5:51:f0 on en0 ifscope [ethernet]
? (172.17.1.108) at 54:4:a6:5:17:d2 on en0 ifscope [ethernet]
? (172.17.1.182) at b0:9f:ba:d:17:d2 on en0 ifscope [ethernet]
? (172.17.1.217) at 10:b:a9:cc:89:2c on en0 ifscope [ethernet]
? (172.17.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
Davids-MacBook-Air-4:~ dave$
```

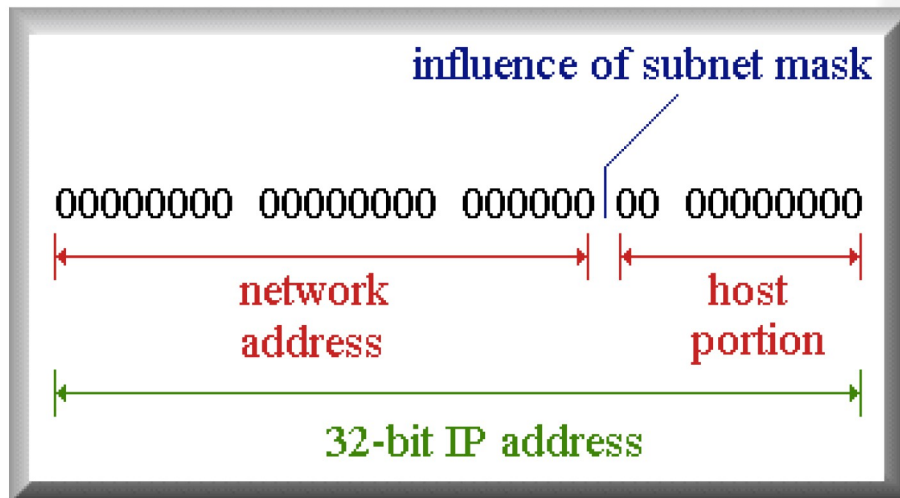
Public versus Private IP addresses

- Your device or gateway must have a globally unique (public) IP address to communicate with hosts outside your local network
- Your router, ISP, or mobile provider may assign a *private-use* IP address to your device



What is a subnet mask?

A number that identifies the number of bits of an IPv4 address that represent the local network identifier



IPv6 prefix numbers serve the same purpose

The remaining bits identify the number of hosts that can be addressed in the local network

Net bits	Subnet mask	total-addresses
/20	255.255.240.0	4096
/21	255.255.248.0	2048
/22	255.255.252.0	1024
/23	255.255.254.0	512
/24	255.255.255.0	256
/25	255.255.255.128	128
/26	255.255.255.192	64
/27	255.255.255.224	32
/28	255.255.255.240	16
/29	255.255.255.248	8
/30	255.255.255.252	4

Try <http://www.tunnelsup.com/subnet-calculator>

Find Your Local IP configuration

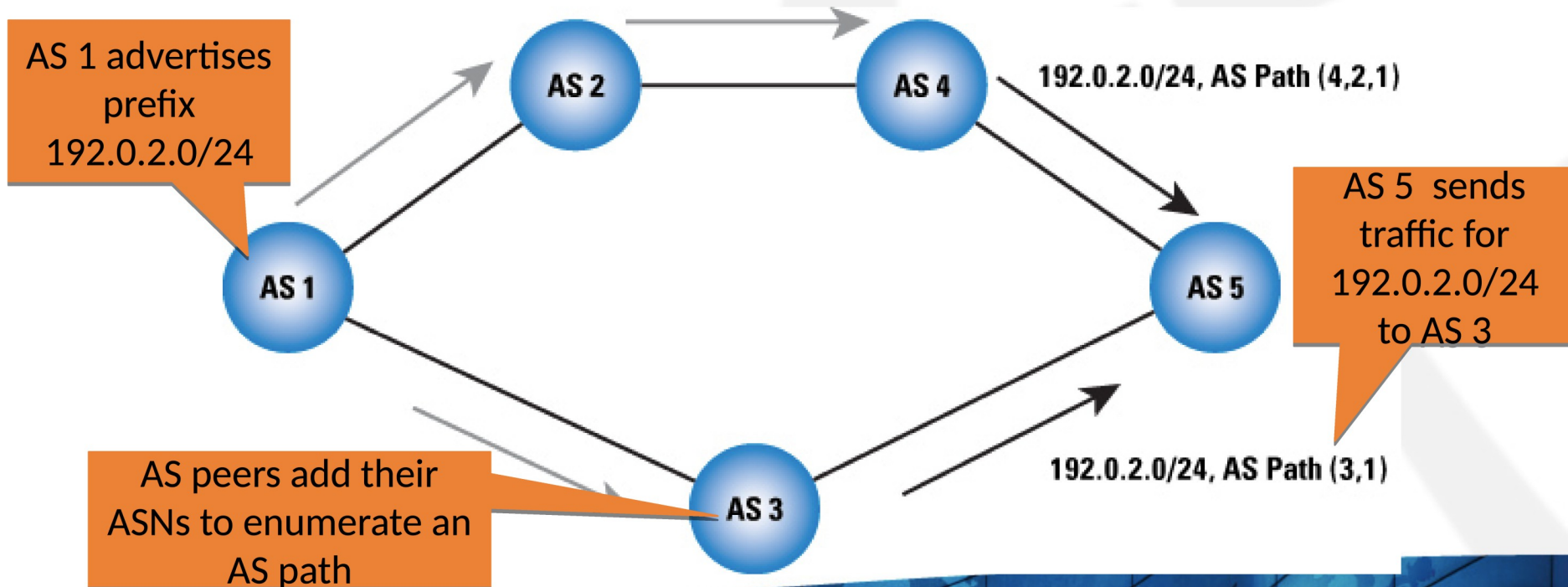
Operating System	Method
Windows Devices	Open cmd.exe, type <i>ipconfig</i>
Open BSD on Mac OS X and Linux	Launch Terminal, type <i>ifconfig</i>
iPhone	Settings -> WiFi, then touch wireless network ID
Android	Settings -> About Tablet -> Status then scroll to <i>Wi-Fi MAC address</i>

Find Your Global IP Address?

- Google “what is my IP?”
- Visit <http://whatismyip.com>

Autonomous System Number (ASN)

- ASNs identify operators who provide Internet access or transit routing service
 - ISPs, cable, mobile providers, hosting/cloud providers...
- AS numbers are used to build global routes



Brief Overview of the DNS

What is the Domain Name System?

A distributed database primarily used to obtain the

IP address, a number, e.g.,
192.168.23.1 or **fe80::226:bbff:fe11:5b32**

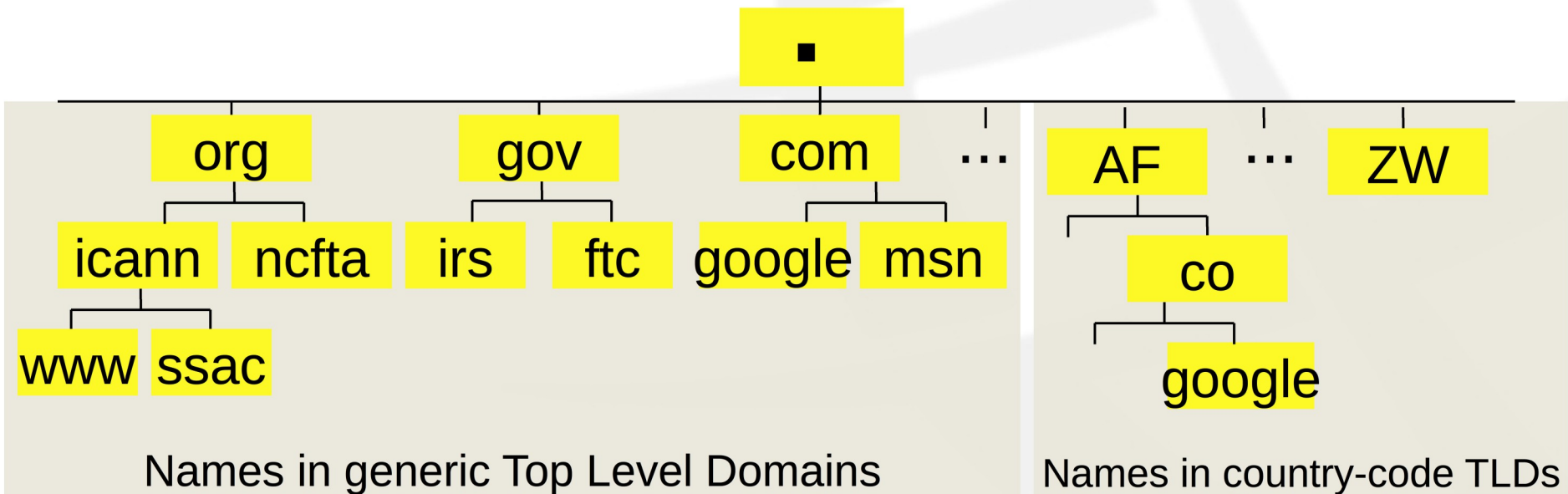
that is associated with a
user-friendly name (www.example.com)

Why do we need a DNS?

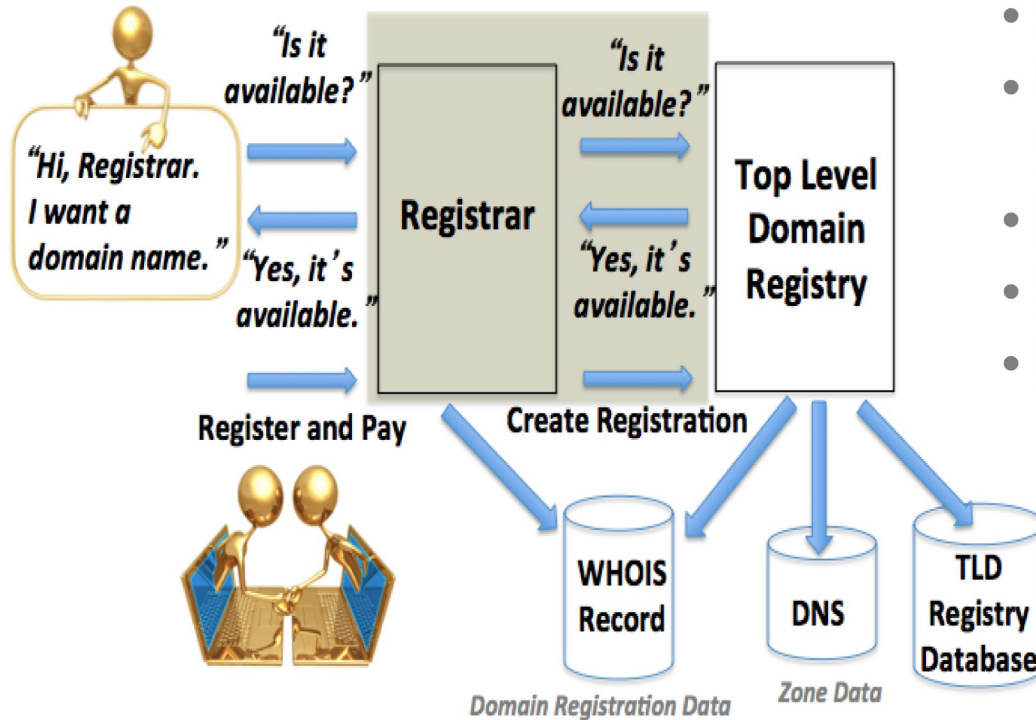
*It's hard to remember lots of four decimal numbers
and it's impossibly hard to remember hexadecimal ones*

What is a domain?

- A **domain** is a node in the Internet name space
 - A domain includes all its descendants
- Domains have names
 - Top-level domain (TLD) names are generic or country-specific
 - TLD *registries* administer domains in the top-level
 - TLD registries *delegate* labels beneath their top level delegation



Domain name registration 101



How to register a domain:

- Choose a string e.g., `example`
- Visit a registrar to check string availability in a TLD
- Pay a fee to register the name
- Submit registration information
- Registrar and registries manage:
 - “string” + TLD (managed in registry DB)
 - Contacts, DNS (managed in Whois)
 - DNS, status (managed in Whois DBs)

Elements of the DNS

- Authoritative Name Servers host zone data
 - The set of “DNS data” that the registrant publishes
- Recursive Name Resolvers (“resolvers”)
 - Systems that find answers to queries for DNS data
- Caching resolvers
 - Recursive resolvers that not only find answers but also store answers locally for “TTL” period of time
- Client or “stub” resolvers
 - Software in applications, mobile apps or operating systems that query the DNS and process responses

What is a DNS zone *data*?

- DNS zone data are hosted at an *authoritative name server*
- DNS zones contain *resource records*
- A resource record (RR) describes
 - name servers,
 - IP addresses,
 - Hosts,
 - Services
 - Cryptographic keys & signatures...

```
$TTL      86400 ; 24 hours could have been written as 24h or 1d
$ORIGIN   example.com.
@ 1D IN    SOA ns1.example.com. hostmaster.example.com. (
                                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 definition
; non server domain hosts
bill IN  A   192.168.0.3
fred IN  A   192.168.0.4
```

US ASCII-7 letters, digits, and hyphens only

Common DNS Resource Records

```
$TTL 86400 ; 24 hours could have been written as 24h or 1d
ORIGIN example.com.
@ 1D IN SOA ns1.example.com. hostmaster.example.com. (
    2002022401 ; serial
    3H ; refresh
    15 ; retry
    1w ; expire
    3h ; minimum
)
IN NS ns1.example.com. ; in the domain
IN NS ns2.example.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 definition
; non server domain hosts
bill IN A 192.168.0.3
fred IN A 192.168.0.4
```

Time to live

- *how long RRs are accurate*

Start of Authority RR contains

- *Source: zone created here*
- *Administrator's email*
- *Revision number of zone file*
- *Zone transfer timers (secondary)*

Name Server (NS)

- *IN (Internet)*
- *Name of authoritative server*

Mail Server (MX)

- *IN (Internet)*
- *Name of mail server*

Common DNS Resource Records

```
$TTL      86400 ; 24 hours could have been written as 24h or 1d
$ORIGIN example.com.
@ 1D IN    SOA ns1.example.com. hostmaster.example.com. (
                                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 definition
; non server domain hosts
bill IN A   192.168.0.3
fred IN A   192.168.0.4
```

Name server address record

- *NS1 (name server name)*
- *IN (Internet)*
- *A (IPv4) * AAAA is IPv6*
- *IPv4 address (192.168.0.1)*

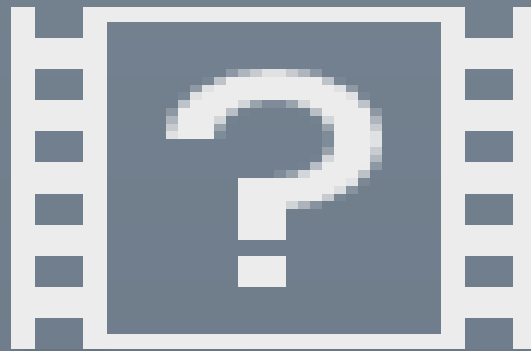
Web server address record

- *www (world wide web)*
- *IN (Internet)*
- *A (IPv4) * AAAA is IPv6*
- *IPv4 address (192.168.0.2)*

File server address record

- *FTP (file transfer protocol)*
- *IN (Internet)*
- *CNAME means “same address spaces and numbers as www”*

Name Resolution Process



How your device finds a resolver: DHCP



Can someone help
me join a
network?



Welcome! I'm your gateway

- My address is 192.168.4.1
- Your IP address is 192.168.4.94
- Your subnet is 255.255.252.0
- Send your DNS queries to the resolver at 192.168.4.1 (me!)

What is caching?

- Iterative resolvers may *cache* DNS records they receive from other name servers as they process client queries
 - Speeds up resolution
 - Saves bandwidth
 - Responses are **non-authoritative**
- Are cached records valid forever?
 - No. The time to live (TTL) field in DNS records bounds how long an iterative resolver can cache that particular record



What is the IPv6 address for
icann.org



I'll cache this
response


icann.org
AAAA 2001:500:88:200::7



Registration Data Directory Services

Whois

Databases containing records of registrations

- 
- Domain Whois
 - Sponsoring Registrar
 - Domain Name Servers
 - Domain Status
 - Creation/Expiry dates
 - Point of Contact
 - DNSSEC data
 - Address Whois
 - Regional Internet Registry
 - IPv4/v6 address allocation
 - ASN allocation
 - Creation/Expiry dates
 - Point of Contact

Relevance to Investigators

Abuse investigations typically involve collection of most/all of these identifiers

- Domain Names
- Name Servers
- IP networks and addresses
- Autonomous Systems
- Registration data

Defining Badness in the DNS

Common Uses for Criminal Domains

- Phishing
- Malware C&C
- Data exfiltration
- Malware distribution (drive-by pages)
- Exploit attacks
- Scams (419, reshipping etc.)
- Counterfeit Goods
- Illegal pharma and piracy
- Infrastructure (ecrime name resolution)



Abuses of other peoples' Domains & DNS

- Criminal hosting infrastructure
- Domain, NS, or MX Hijacking
- Hacktivism (e.g., defacement)
- Tunneling/Beaconing for covert comms
- Attack obfuscation
- Host file modification (infected devices)
- Changing default resolvers (DNSChanger)
- Poisoning (resolver/ISP)
- Traffic diversion
- MITM attacks (insertion, capture)

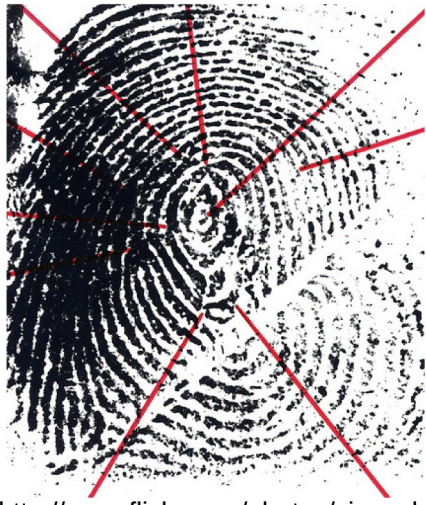
How criminals acquire DNS resources

- Purchase using stolen credit cards, compromised accounts
- Exploit “free” services
- Leverage bullet-proof or grey hat hosting/domain providers
- Hack and exploit legitimate hosts
- Phish account credentials and use to register/configure new

Is this an Abuse (Malicious) Domain or A Misused Domain?

Not always easy to differentiate

Determining factors for DNS Abuse/Misuse



<http://www.flickr.com/photos/vincealongi/>

- Recent domain registration creation date
- Base site content is non-existent or bad
- Spoofing or confusing use of a brand
- Known DGA or malware control point
- Questionable Whois contact data
- Privacy protection service
- Suspicious or notorious name servers
- Suspicious or notorious hosting location
- High frequency/volume of Name errors
- Suspicious values in DNS Zone data (e.g., TTL)

Not always easy to identify badness

- Criminals Use Obfuscation
 - Redirection: hacked sites use URL shorteners
 - Recursion: Shortened URLs are shortened
 - One-time use URLs
 - Add subdomains to zone at a hacked DNS server
 - Country- or script-specific content
 - Privacy-protected domain registrations or bogus Whois
- Criminals use ACLs
 - Prevent registrars, Google, LE, investigators from seeing sites
- “Criminal” behaviors can emulate legitimate behavior
 - EXAMPLE: Fast flux versus adaptive networking (e.g., CDNs)

Investigating an “abuse” domain

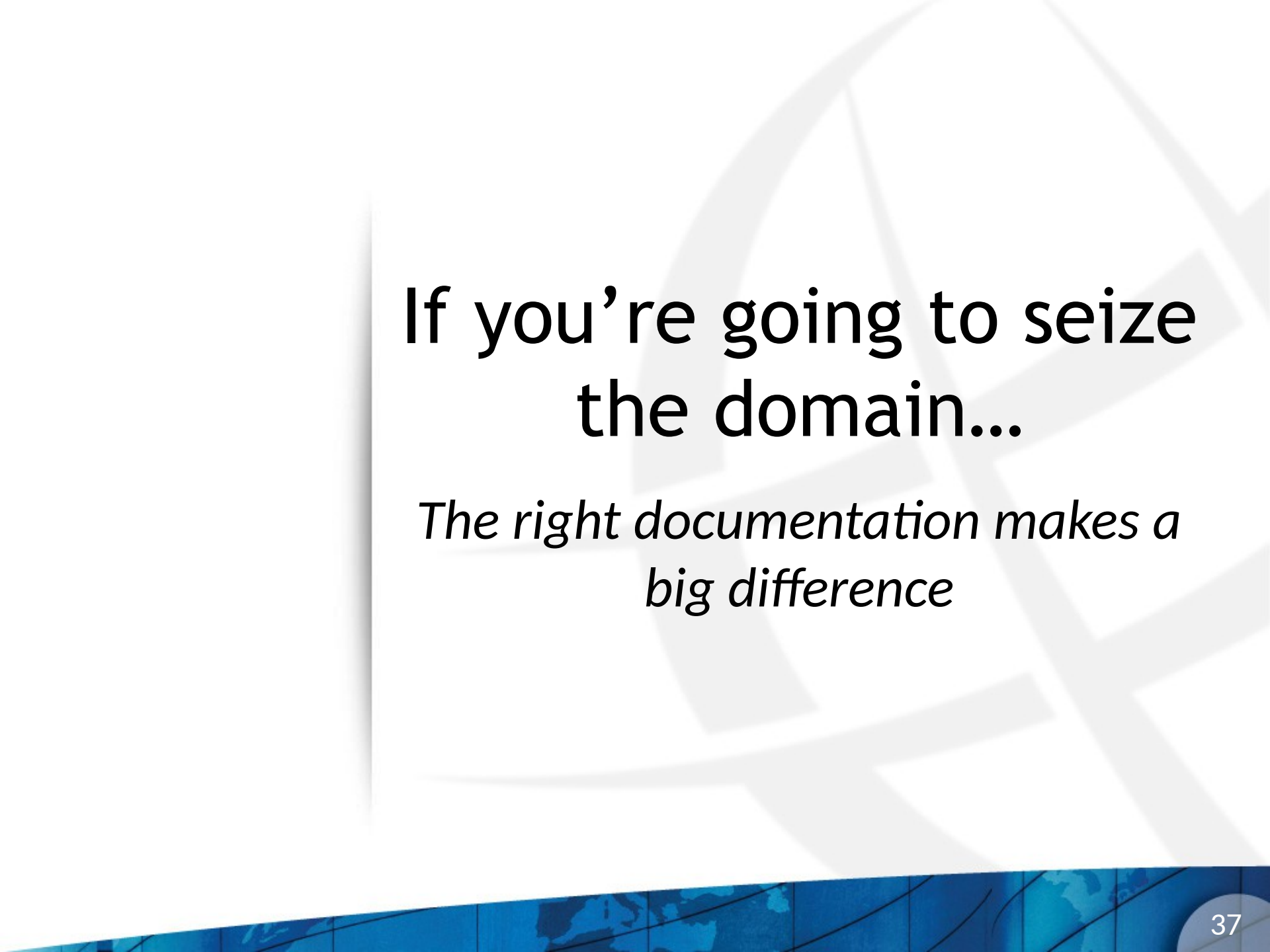
1. Collect evidence of abuse
 - A. The purpose of this course is to show ways to do this
2. Determine registrar
 - A. Is there a reseller of that registrar involved?
3. Contact registrar abuse desk
 - A. Provide evidence of abuse
 - B. Point out registration problems
 - C. Ask if TOS ,ICANN, ccTLD registry domain suspension policy applies
4. No success? Contact registry
 - A. Same supporting info as registrar
5. Escalate
 - A. NX-Domains
 - B. WDPRS and/or ACPA (US-based)
 - C. ICANN compliance if WDPRS is ignored
 - D. National CERT or local LE
 - E. Sharing/intel networks

If you are looking at a suspicious domain, someone else is, too.

Collecting Evidence of Abuse/Misuse

- Domain names
- Name servers, resolvers
- DNS zone data
- DNS traffic
- Name registration data
- Registry, Registrar
- Registrar
- Host IP addresses
- IP networks
- Address registration data
- Autonomous systems
- Service providers
- Hosting providers
- Hosted content

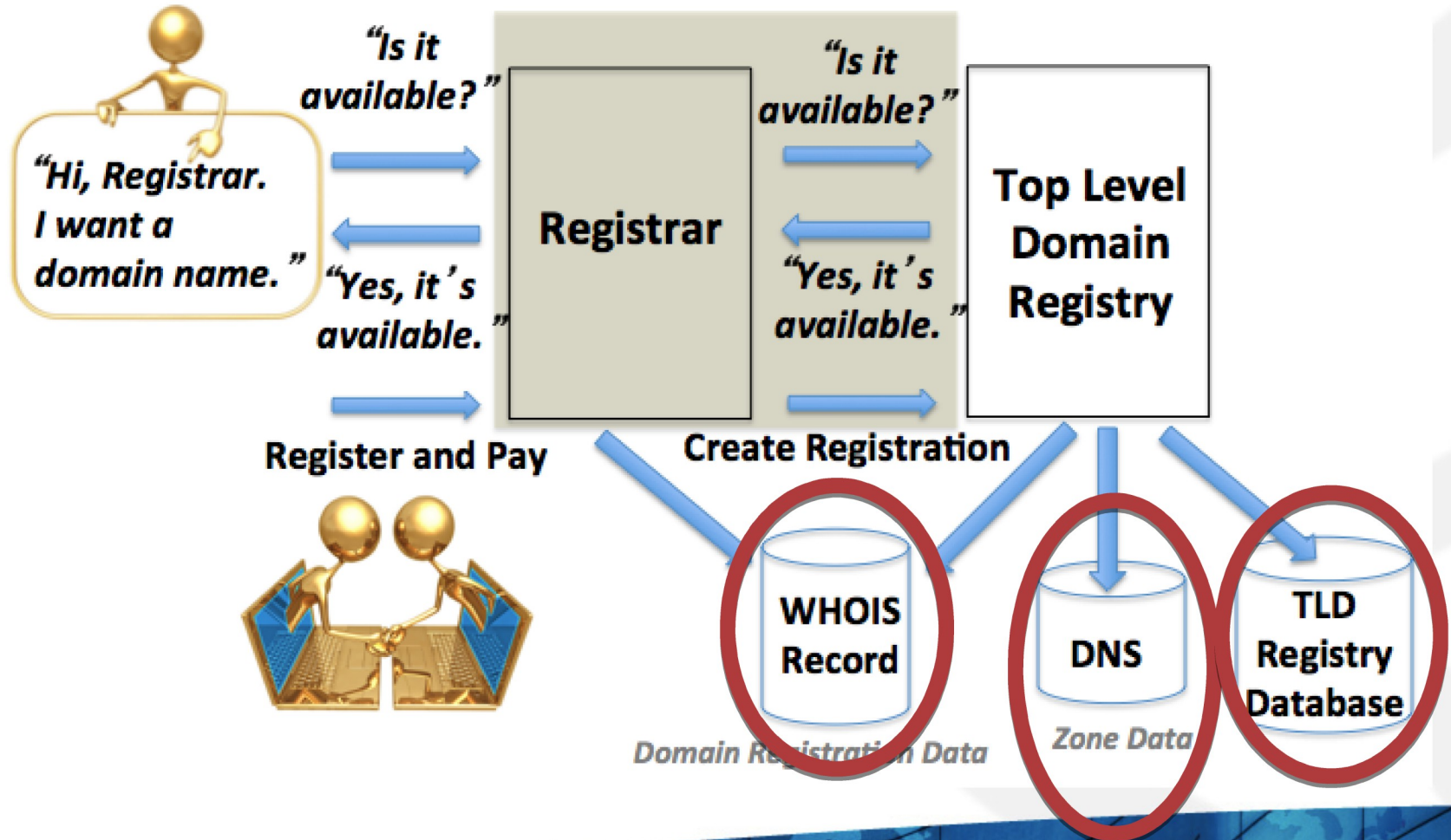
R e p u t a t i o n



If you're going to seize
the domain...

*The right documentation makes a
big difference*

Seizures affect several Internet name databases and operations



Relevance



All of this information is relevant in some way when an order or warrant is issued

(list of) domain name(s) identifies

- Registries that are obliged to act on the order

Registration data ("Whois") identifies

- sponsoring registrar
- party alleged to "own" the domain
- servers that provide DNS (name resolution)
- "status" of the domain

Questions to consider when preparing an order: context

- Who is making the request?
 - Plaintiff, defendant, court of record
 - Who are the primary points of contact?
 - Can registry/registrar readily verify the request?
- What kind of request is this?
 - Court order or 3rd party request for action?
- What is the expected response time?

Questions to consider when preparing an order: Registration

- Is there a desire to obtain records?
- Is the domain name to be transferred to a different sponsoring registrar?
- Are you transferring the registration? To whom?
- What status should the registry set for the domain?
 - E.g., prevent transfer, update, or delete?
- What should WHOIS for the domain name display?

Questions to consider when preparing an order: DNS operations

- How should DNS respond to queries for seized domains?
 - Is name resolution service (DNS) to be suspended?
 - Is redirection to a text of notice page required?
 - Is redirection of Internet hosting required?
- Who will operate DNS for seized domains?
 - Is the party that provides name resolution service (DNS) to be changed?

What should you consider to minimize collateral harm?

Examples of questions to ask before you file:

- Will your action disrupt
 - Name service for other (reputable) domains?
 - Hosting services for parties other than those named in your order?
- What services other than web are affected by your action on the domain name?
- What do you expect as the “long term disposition” of the domain name?
- Could your actions interfere with other active investigations, monitoring, surveillance... ?

Tools for Investigating Badness

*DNS... domain registrations...
name servers... hosting...
content... reputation.*

Tools for Investigators

- Many tools to help you you identify the abused or malicious resource
 - Domain names, host names, IP addresses, ASNs
 - Hosting location (web, DNS, mail) or origin
 - Content (URL, file, email, attachment)
- Many tools to identify whom to contact or report the resource
 - Databases of domain registrants, operators, ISPs
 - Block list and analysis sites and data providers

Web based Whois tools



Whois Record for SecuritySkeptic.com

Related Domains For Sale or At Auction

[SkepticsSociety.com](#) (\$2,388) [RationalSkepticism.com](#) (\$1,688)
[ClimateSkeptic.com](#) (\$2,595) [BibleSkeptic.com](#) (\$1,895)
[YoungSkeptics.com](#) (\$1,095) [WebSkeptic.com](#) (\$795)

Whois & Quick Stats

Registrant Org	Core Competence is associated with ~1 other domains	↗
Registrar	GODADDY.COM, LLC	
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited	
Dates	Created on 2007-02-27 - Expires on 2015-02-27 - Updated on 2013-02-12	↗
IP Address	141.101.115.9 - 17,244 other sites hosted on this server	↗
Name Server(s)	NS25.DOMAINCONTROL.COM (has 37,171,396 domains) NS26.DOMAINCONTROL.COM (has 37,171,396 domains)	↗
IP Location	🇺🇸 - Virginia - West Mclean - Cloudflare Cdn Network	
ASN	🇺🇸 AS13335 CLOUDFLARENET - CloudFlare, Inc.,US (registered Jul 14, 2010)	
Domain Status	Registered And Active Website	
Whois History	28 records have been archived since 2007-12-	↗



Domain Dossier Investigate domains and IP addresses

domain or IP address

☒ domain whois record ☐ DNS records ☐ traceroute
☐ network whois record ☐ service scan

user: anonymous [174.107.217.54]

balance: 45 units

[log in](#) | [account info](#)

Central Ops .net

Address lookup

canonical name [google.com.](#)

aliases

addresses **2a00:1450:4002:801::1001**
173.194.35.9
173.194.35.14
173.194.35.0
173.194.35.1
173.194.35.2
173.194.35.3
173.194.35.4
173.194.35.5
173.194.35.6
173.194.35.7
173.194.35.8

Domain Whois record


Queried [whois.internic.net](#) with "dom google.com"...


Domain Name: GOOGLE.COM
Registrar: MARKMONITOR INC.
Whois Server: whois.markmonitor.com
Referral URL: http://www.markmonitor.com
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM

Tools for Investigating Registrations


- **Whois Port 43 clients, command line executables**
<http://whois.software.informer.com/download-whois-msdos/>
- **Delegation Records for ccTLD and new TLDs**
http://www.101domain.com/domain_whois_server.php
<http://newgtlds.icann.org/en/program-status/delegated-strings>

DOMAIN WHOIS SERVER





[LA Home](#)
[Domain Information](#)
[TLD Back Search](#)
[Whois](#)
[Renewals](#)
[Transfers](#)
[Hosting](#)
[SSL](#)
[Email Services](#)
[FAQ](#)



L - Whois Server

- [La Land](#)
- [Land Land](#)
- [Lat Latino](#)
- [Latino Latino](#)
- [Law Law](#)
- [Lawyer Lawyer](#)
- [Le Lebanon](#)
- [Le Saint Lucia](#)
- [Lesson Lesson](#)
- [Legal Legal](#)
- [Legal Lesbian Gay Bisexual Transgender](#)
- [Li Lithuania](#)
- [Life Life](#)
- [Life Insurance Life Insurance](#)
- [Lighting Lighting](#)
- [Limited Liability Company](#)
- [Link Link](#)
- [Link Link](#)
- [List List](#)

Delegation Record

For .la Laos

Domain Registration, la

Sponsoring Organization

Lao National Internet Committee (LANIC)
 Science Technology and Environment Agency
 Prime Ministry's Office
 P.O. Box 2279
 Vientiane Lao PDR
 Lao People's Democratic Republic

Sub Domains

Administrative Contact

Mr. Nourin SHANHANTHIT
 Lao National Internet Committee (LANIC)
 Prime Ministry's Office
 P.O. Box 2279
 Vientiane Lao PDR
 Lao People's Democratic Republic
 Email: admincontact@lanic.net
 Fax: +856 21 213470
 Fax: +856 21 13472

Technical Contact

Mr. Maydom CHANTHANASINH
 Lao National Internet Committee (LANIC)
 Prime Minister's Office
 P.O. Box 2279
 Vientiane Lao PDR
 Lao People's Democratic Republic
 Email: technicalcontact@lanic.net
 Fax: +856 21 213470
 Fax: +856 21 213472

Name Servers

Tools for Investigating DNS

- dig (Linux, BSD, MacOS), nslookup (Win), host
<http://support.microsoft.com/kb/200525>
<https://library.linode.com/linux-tools/common-commands/dig>
- Domain Dossier
<http://centralops.net/co/DomainDossier.aspx>
- Robtex
<http://www.robtex.com/dns/>
- Passive DNS
http://www.bfk.de/bfk_dnslogger.html

Using dig (Linux, BSD)

davepiscitello — bash — 80x24

```
Last login: Wed Aug 8 17:13:30 on console
Daves-MacBook-Pro:~ davepiscitello$ man dig
Daves-MacBook-Pro:~ davepiscitello$ dig icann.org
```

```
; <<>> DiG 9.8.1-P1 <<>> icann.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7037
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
icann.org.                IN      A

;; ANSWER SECTION:
icann.org.                600     IN      A      192.0.43.7

;; Query time: 67 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Aug 21 12:24:26 2012
;; MSG SIZE rcvd: 43
```

basic dig

```
Daves-MacBook-Pro:~ davepiscitello$
Daves-MacBook-Pro:~ davepiscitello$
```

davepiscitello — bash — 80x24

```
Daves-MacBook-Pro:~ davepiscitello$ dig icann.org +noadditional
```

```
; <<>> DiG 9.8.1-P1 <<>> icann.org +noadditional
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24467
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
```

```
;; QUESTION SECTION:
icann.org.                IN      A

;; ANSWER SECTION:
icann.org.                344     IN      A      192.0.43.7
```

```
;; Query time: 46 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Aug 21 12:28:42 2012
;; MSG SIZE rcvd: 43
```

```
Daves-MacBook-Pro:~ davepiscitello$
```

suppress additional section

davepiscitello — bash — 80x24

```
Daves-MacBook-Pro:~ davepiscitello$ dig -t MX icann.org +noquestion +nocomments +nostats
```

```
; <<>> DiG 9.8.1-P1 <<>> -t MX icann.org +noquestion +nocomments +nostats
;; global options: +cmd
icann.org.                536     IN      MX      10 pechora1.icann.org.
icann.org.                536     IN      MX      10 pechora2.icann.org.
icann.org.                536     IN      MX      10 pechora3.icann.org.
icann.org.                536     IN      MX      10 pechora4.icann.org.
icann.org.                536     IN      MX      10 pechora5.icann.org.
icann.org.                536     IN      MX      10 pechora6.icann.org.
icann.org.                536     IN      MX      10 pechora7.icann.org.
icann.org.                536     IN      MX      10 pechora8.icann.org.
```

```
Daves-MacBook-Pro:~ davepiscitello$
```

ask for mail servers

davepiscitello — bash — 80x24

```
Daves-MacBook-Pro:~ davepiscitello$ dig -t NS icann.org +noquestion +nocomments +nostats
```

```
; <<>> DiG 9.8.1-P1 <<>> -t NS icann.org +noquestion +nocomments +nostats
;; global options: +cmd
icann.org.                22412   IN      NS      a.iana-servers.net.
icann.org.                22412   IN      NS      b.iana-servers.net.
icann.org.                22412   IN      NS      c.iana-servers.net.
icann.org.                22412   IN      NS      d.iana-servers.net.
icann.org.                22412   IN      NS      ns.icann.org.
```

```
Daves-MacBook-Pro:~ davepiscitello$
```

ask for name servers

ain internet groper

Using nslookup (MS-DOS)

```
C:\>C:\WINDOWS\system32\cmd.exe
```

```
C:\>nslookup icann.org
Server: google-public-dns-a.google.com
Address: 8.8.8.8
```

basic nslookup

```
Non-authoritative answer:
Name: icann.org
Address: 192.0.43.7
```

```
C:\>nslookup -querytype=MX icann.org
Server: google-public-dns-a.google.com
Address: 8.8.8.8
```

ask for mail servers

```
Non-authoritative answer:
icann.org MX preference = 10, mail exchanger = pechora4.icann.org
icann.org MX preference = 10, mail exchanger = pechora5.icann.org
icann.org MX preference = 10, mail exchanger = pechora6.icann.org
icann.org MX preference = 10, mail exchanger = pechora7.icann.org
icann.org MX preference = 10, mail exchanger = pechora8.icann.org
icann.org MX preference = 10, mail exchanger = pechora1.icann.org
icann.org MX preference = 10, mail exchanger = pechora2.icann.org
icann.org MX preference = 10, mail exchanger = pechora3.icann.org
```

```
C:\>nslookup -q=NS icann.org
Server: google-public-dns-a.google.com
Address: 8.8.8.8
```

ask for name servers

```
Non-authoritative answer:
icann.org nameserver = a.iana-servers.net
icann.org nameserver = b.iana-servers.net
icann.org nameserver = c.iana-servers.net
icann.org nameserver = d.iana-servers.net
icann.org nameserver = ns.icann.org
```

```
C:\>nslookup -q=aaaa icann.org
Server: google-public-dns-a.google.com
Address: 8.8.8.8
```

ask for IPv6 addresses

```
Non-authoritative answer:
icann.org AAAA IPv6 address = 2001:500:88:200::7
```

```
C:\>nslookup -q=any icann.org
Server: google-public-dns-a.google.com
Address: 8.8.8.8
```

```
Non-authoritative answer:
icann.org
primary name server = dns1.icann.org
responsible mail addr = hostmaster.icann.org
serial = 2012082006
refresh = 10800 (3 hours)
retry = 3600 (1 hour)
expire = 1209600 (14 days)
default TTL = 3600 (1 hour)
icann.org ??? unknown type 46 ???
icann.org nameserver = ns.icann.org
icann.org nameserver = c.iana-servers.net
icann.org nameserver = d.iana-servers.net
icann.org nameserver = b.iana-servers.net
icann.org nameserver = a.iana-servers.net
icann.org ??? unknown type 46 ???
icann.org internet address = 192.0.43.7
icann.org ??? unknown type 46 ???
icann.org MX preference = 10, mail exchanger = pechora3.icann.org
icann.org MX preference = 10, mail exchanger = pechora4.icann.org
icann.org MX preference = 10, mail exchanger = pechora5.icann.org
icann.org MX preference = 10, mail exchanger = pechora6.icann.org
icann.org MX preference = 10, mail exchanger = pechora7.icann.org
icann.org MX preference = 10, mail exchanger = pechora8.icann.org
icann.org MX preference = 10, mail exchanger = pechora1.icann.org
icann.org MX preference = 10, mail exchanger = pechora2.icann.org
icann.org ??? unknown type 46 ???
icann.org AAAA IPv6 address = 2001:500:88:200::7
icann.org ??? unknown type 46 ???
icann.org ??? unknown type 48 ???
icann.org ??? unknown type 48 ???
icann.org ??? unknown type 48 ???
icann.org ??? unknown type 48 ???
icann.org ??? unknown type 48 ???
icann.org ??? unknown type 48 ???
icann.org ??? unknown type 46 ???
icann.org ??? unknown type 51 ???
icann.org ??? unknown type 46 ???
```

ask for "any"

name system lookup

Web based DNS tool: Domain Dossier

masterbayi.com - Domain Dossier - owner and registrar information, whois and DNS records

masterbayi.com - Domain Dossier

centralops.net/co/DomainDossier.aspx

Domain Dossier

Investigate domains and IP addresses

domain or IP address

☐ domain whois record ☒ DNS records ☐ traceroute

☐ network whois record ☐ service scan

user: anonymous [174.107.217.54]
balance: 45 units
[log in](#) | [account info](#)

Central Ops - net

Address lookup

canonical name **masterbayi.com.**

aliases

addresses **88.150.242.188**

DNS records

name	class	type	data	time to live
masterbayi.com	IN	MX	preference: 0 exchange: masterbayi.com	14400s (04:00:00)
masterbayi.com	IN	SOA	server: ns1.masterbayi.com email: m@m.com serial: 2013072202	86400s (1.00:00:00)

Find: ☐ Highlight all ☐ Match case

malicious chrome extension - can anyone here get it pulled?

found this by way of a redirect posted to facebook

hxxp://b-1.cc/R4zy?25650

redir to

hxxp://masterbayi.com/index1.php

MALICIOUS EXTENSION <https://chrome.google.com/webstore/detail/video-plus/penapfmchkoamhbjlohlhpghopnielhd>

Excerpt from email

Let's see what's in the zone...

Web based DNS tool: Robtex

in:spam

← Delete forever Not spam More

Wholesale Watches - www.AkzanWholesale.com - Factory Direct . Free Shipping! Huge Selection.

View Our Wholesale Rolex Replica watches Today

Spam x

Xavier Culver bobby.wood@wrightind.com via 5:56 PM (0 minutes ago) ☆

to dave

Why is this message in Spam? It contains content that's typically used in spam messages. [Learn more](#)

Hello Dave

She won't be competent to take her eyes off your wrist!
If you want to find the present you wish the one who it's for will like – visit Prestige and you will see here presents that will never be named as unneeded.

I am very happy to say my Gucci watch arrived in the mail today and i am very pleased with it thank you so much for sending so fast and i will recommend your website to my friends.
Thanks - Everything's great!
Xavier Culver

Click here → <http://ptall.ru>

Where is this spam URL taking us?

ptall.ru

dns.robtex.com/ptall.ru.html#summary

Result Summary Records Graph Shared Whois Blacklists Analysis Contact

ptall.ru

Lucky Search

Google Custom Search

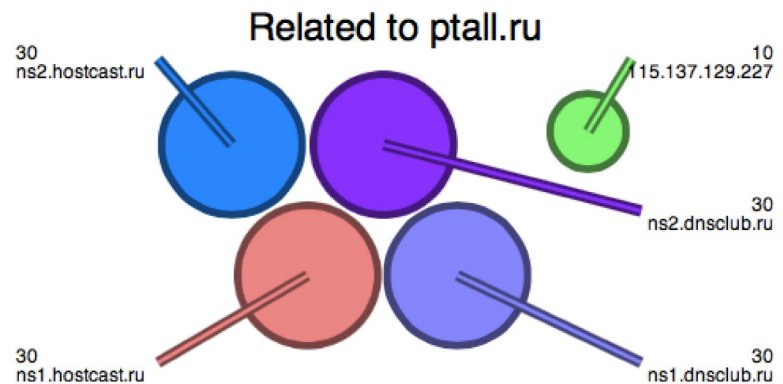
Like 0 +1 0

Tweet 0

Summary

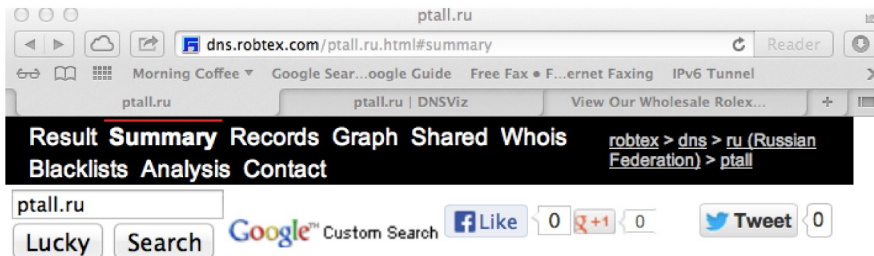
Zunde.ru, dosepilldrugstore.ru, rxpharmacytabletsipills.ru, pharmacypharmacyrx.ru, acild.ru and at least two other hosts point to the same IP. Deace.ru, kravo.ru, hainy.ru, borag.ru, arota.ru and at least 25 other hosts share name servers with this domain.

Also check www.ptall.ru.



<http://dns.robtex.com/ptall.ru.html#summary>

Robtex



The name server ns1.hostcast.ru

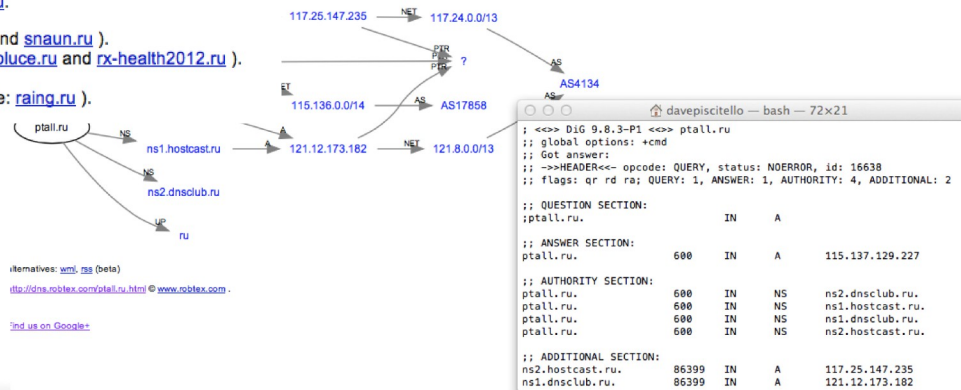
There are about thirty domains that use the name server [ns1.hostcast.ru](#).

- All of those use the four name servers [ns1.dnscub.ru](#), [ns2.dnscub.ru](#), [ns1.hostcast.ru](#) and [ns2.hostcast.ru](#) together, hereafter referred to as "name server group 1", (example: [sagil.ru](#), [aunie.ru](#) and [senky.ru](#)).
- Nine of them point only to the IP number [124.51.247.59](#) (example: [ascep.ru](#), [vaise.ru](#) and [bdram.ru](#)).
- Seven of them point only to the IP number [119.1.109.72](#) (example: [moord.ru](#), [bamen.ru](#) and [gondl.ru](#)).
- Four of them point only to the IP number [89.103.247.114](#) (example: [mahen.ru](#), [omict.ru](#) and [axies.ru](#)).

The name server ns2.hostcast.ru

There are about thirty domains that use the name server [ns2.hostcast.ru](#).

- All of those use name server group 1 (example: [kneah.ru](#), [tusus.ru](#) and [snaun.ru](#)).
- Nine of them point only to the IP number [124.51.247.59](#) (example: [bluce.ru](#) and [rx-health2012.ru](#)).
- Seven of them point only to the IP number [119.1.109.72](#).
- Four of them point only to the IP number [112.216.242.125](#) (example: [raing.ru](#)).



Graph (compare to dig output)
<http://dns.robtex.com/ptall.ru.html#graph>

Passive DNS Replication (PDNS)

- Basics:
 - Monitor DNS queries & responses (near recursive servers)
 - Put all of these data in a database
 - Query database to extract behavior
- PDNS shows query and response traffic
 - DNS records clients are asking to resolve
 - Responses resolvers receives back from authoritative servers
- Best results at big ISPs
 - Physical network location with visibility
 - Filter down to just the DNS queries/responses

Queryable PDNS Collections

- BFK
 - http://www.bfk.de/bfk_dnslogger.html
- SIE (ISC)
- DNSParse (Bojan)
 - <http://dnsparse.insec.auckland.ac.nz/dns/>
- DNSDB
 - <https://www.dnsdb.info/>
- GitHub
 - <https://github.com/chrislee35/passivedns-client>

Investigating using PDNS

What name server hosts zone for the reported abuse domain?

The image shows two browser windows. The top window is SpamCop.net, displaying a list of abuse reports. The bottom window is BFK edv-consulting GmbH, showing the 'Passive DNS replication' section with a search query.

SpamCop.net - inprogress

60 issues
38 recipients

Abuse report sent to

nomaster@devnull.spamcop.net
nomaster@devnull.spamcop.net
nomaster@devnull.spamcop.net
nomaster@devnull.spamcop.net

Age

1.42 min. <http://nzrqd.shadeespecial.pl.ua/>
1.42 min. <http://zelth.shadeespecial.pl.ua/>
1.42 min. <http://mdkmq.shadeespecial.pl.ua/>
1.42 min. <http://mdwee.shadeespecial.pl.ua/>

Reported web site

BFK edv-consulting GmbH - Sicher

Find: Next Previous Highlight all Match case

Features

Passive DNS replication

As a service to CERTs and incident response teams, BFK uses passive DNS replication to collect public DNS data. Compared to the ordinary domain name system, this database adds further search capabilities. This web interface **must not** be used for automated queries. For details about bulk queries please contact: dnslogger-ops@bfk.de

Query: submit

The server returned the following data:

shadeespecial.pl.ua	NS	ns1.tionhost.com
shadeespecial.pl.ua	NS	ns2.tionhost.com

Find: Next Previous Highlight all Match case

And PDNS says...

Investigating using PDNS

Additional data may be available with this query: [tionhost.com](#)

The server returned the following data:

rememb.pl.ua	NS	ns1.tionhost.com
shinec.pl.ua	NS	ns1.tionhost.com
bcheste.pl.ua	NS	ns1.tionhost.com
solek.pl.ua	NS	ns1.tionhost.com
shadeespecial.pl.ua	NS	ns1.tionhost.com
shinw.pl.ua	NS	ns1.tionhost.com
severegrow.pl.ua	NS	ns1.tionhost.com
tionhost.com	NS	ns1.tionhost.com
ns1.tionhost.com	A	60.173.26.28
ns1.tionhost.com	A	116.255.233.200
doctordia.ru	NS	ns1.tionhost.com
doctormala.ru	NS	ns1.tionhost.com
doctorora.ru	NS	ns1.tionhost.com
medicbuzza.ru	NS	ns1.tionhost.com
doctorbab.ru	NS	ns1.tionhost.com
doctorchoc.ru	NS	ns1.tionhost.com
medicstitc.ru	NS	ns1.tionhost.com
doctorcuc.ru	NS	ns1.tionhost.com
doctordad.ru	NS	ns1.tionhost.com
doctortoad.ru	NS	ns1.tionhost.com
doctorneed.ru	NS	ns1.tionhost.com
doctorrod.ru	NS	ns1.tionhost.com

The server returned the following data:

rememb.pl.ua	A	46.161.41.114
rememb.pl.ua	A	46.161.41.115
rememb.pl.ua	A	78.46.105.79
rememb.pl.ua	A	123.157.149.15
rememb.pl.ua	NS	ns1.tionhost.com
rememb.pl.ua	NS	ns2.tionhost.com

The server state is: 201 Okay

Next... Start looking at IPs and ASNs

Tools for Investigating IP Addresses

- RIR IP Whois
 - ARIN, RIPE, APNIC, , AfrinIC, LACNIC
- Shadowserver Whois
 - <http://www.shadowserver.org/wiki/pmwiki.php/Services/IP-BGP>
- Robtex.com
- Sameip.net
- DNSSTuff
 - <http://www.dnsstuff.com>

Investigating & Locating IP addresses

46.161.41.114 is
In AS6849

Origin AS Data		RIR Data	
ASN	6849	Reverse	NA
Name	UKRTELNET	Reverse-verified	NA
Description	JSC UKRTELECOM,	Origin AS	JSC UKRTELECOM,
# Peers	3	Country Code	RU
# IPv4 Origin Ranges	30	Country	Russia
# IPv6 Origin Ranges	0	Region	Asia
Registrar	RIPE-NCC	Population	145470197
	Nov 29, 1996	Top-level Domain	RU
	UA	IPv4 Ranges	6256
		IPv6 Ranges	424
		Currency	Russian Ruble
		Currency Code	RUB
		IP Range - Start	46.161.0.0
		IP Range - End	46.161.63.255
		Registrar	RIPE-NCC
		Allocation date	Nov 16, 2010

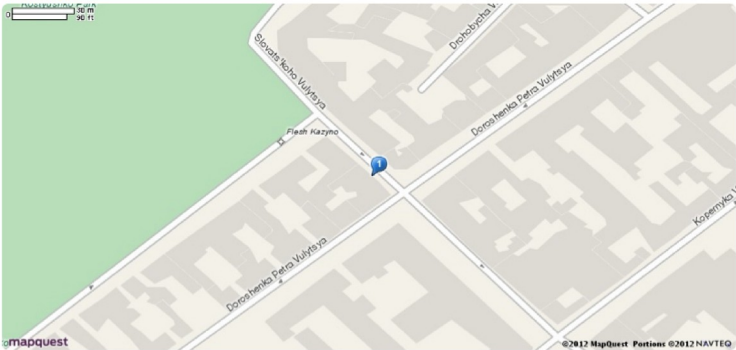
Toolbox | DNSstuff

www.dnsstuff.com/tools#ipinformation/type=domain&value=46.161.41.114

IP Information Results for 46.161.41.114

Country	Country Code	Region	City	Latitude	Longitude	ISP
UKRAINE	UA	L'VIVSKA OBLAST'	L'VIV	49.838261	24.023239	PETERSBURG INTERNET ...

Geolocation Data



mapquest

©2012 MapQuest Portions ©2012 NAVTEQ

Find: trace

Next Previous Highlight all Match case

Mapping IP to BGP prefixes and ASNs

Whois/Origin



```
$ whois -h asn.shadowserver.org origin 17.112.152.32
714 | 17.112.0.0/16 | APPLE-ENGINEERING | US | APPLE.COM | APPLE COMPUTER INC
```

The output is as follows

ASN	Prefix	AS Name	CN	Domain	ISP
-----	--------	---------	----	--------	-----

Whois/Peer

Using the *peer* mode is very similar:

```
$ whois -h asn.shadowserver.org peer 17.112.152.32
3356 7018 | 714 | 17.112.0.0/16 | APPLE-ENGINEERING | US | APPLE.COM | APPLE COMPUTER INC
```

The output is as follows

Peer(s)	ASN	Prefix	AS Name	CN	Domain	ISP
---------	-----	--------	---------	----	--------	-----

A more verbose mode is also available:

```
$ whois -h asn.shadowserver.org peer 4.5.6.4 verbose
3356 | 4.0.0.0/9 | LEVEL3 | US | DSL-VERIZON.NET | GTE.NET LLC


209      ASN-QWEST      Qwest
293      ESNET          Energy Sciences Network
701      UUNET          MCI Communications Services, Inc. d/b/a Verizon Business
702      AS702          Verizon Business EMEA - Commercial IP service provider in Europe
1239     SPRINTLINK     Sprint
1668     AOL-ATDN       AOL Transit Data Network
2497     JPNIC-ASBLOCK  AP JPNIC
2828     XO-AS15        XO Communications
```

Investigating ASNs

Toolbox | DNSstuff | Team Cymru IP to ASN Lookup ...

https://asn.cymru.com/cgi-l

Team Cymru IP to ASN Lookup v1.0

 [CYMRU] [ASN LOOKUP] [HTTP(S) ASN LOOKUP]

Family: ☒ IPv4 ☐ IPv6 Methods: ☒ whois ☒ peer-whois

Flags: ☐ prefix ☐ cc ☐ registry ☐ allocated ☐ nottruncate ☐ verbose

46.161.41.114

Insert your IP or ASN in the textbox above.

Executing commands. Please be patient!

v4.whois.cymru.com

The server returned 4 line(s).

```
[Querying v4.whois.cymru.com]
[v4.whois.cymru.com]
AS      IP      AS Name
6849    46.161.41.114    UKRTELNET JSC UKRTELECOM,
```

v4-peer.whois.cymru.com

The server returned 6 line(s).

```
[Querying v4-peer.whois.cymru.com]
[v4-peer.whois.cymru.com]
PEER_AS  IP      AS Name
1299     46.161.41.114    TELIANET TeliaNet Global Network
3356     46.161.41.114    LEVEL3 Level 3 Communications
3549     46.161.41.114    GBLX Global Crossing Ltd.
```

Get ASN that advertises
IP network of abuse domain

Get ASNs of providers
that peer...

Get PoCs from IP Whois

Whois-RWS

Toolbox | DNSstuff | Whois-RWS

whois.arin.net/rest/asn/AS6656/pft

WHOIS-RWS

ARIN Online enter

Autonomous System Number	
Number	6656 - 6911
Name	RIPE-188-BLOCKS
Handle	AS6656
Organization	RIPE Network Coordination Centre (RIPE)
Registration Date	1996-05-15
Last Updated	2003-04-25
Comments	These addresses have been further assigned to users in the RIPE NCC region. Contact information can be found in the RIPE database at http://www.ripe.net/whois
RESTful Link	http://whois.arin.net/rest/asn/AS6656
See Also	Organization's POC records.

Find: trace Next Previous Highlight all Match case

<https://asn.cymru.com/>

Tools for Investigating Reputation

Reputation services, Block lists, Malware Analysis

Spamhaus

SURBL

ZeusTracker

Team Cymru

Alexa

Clean MX

CBL

Stopbadware

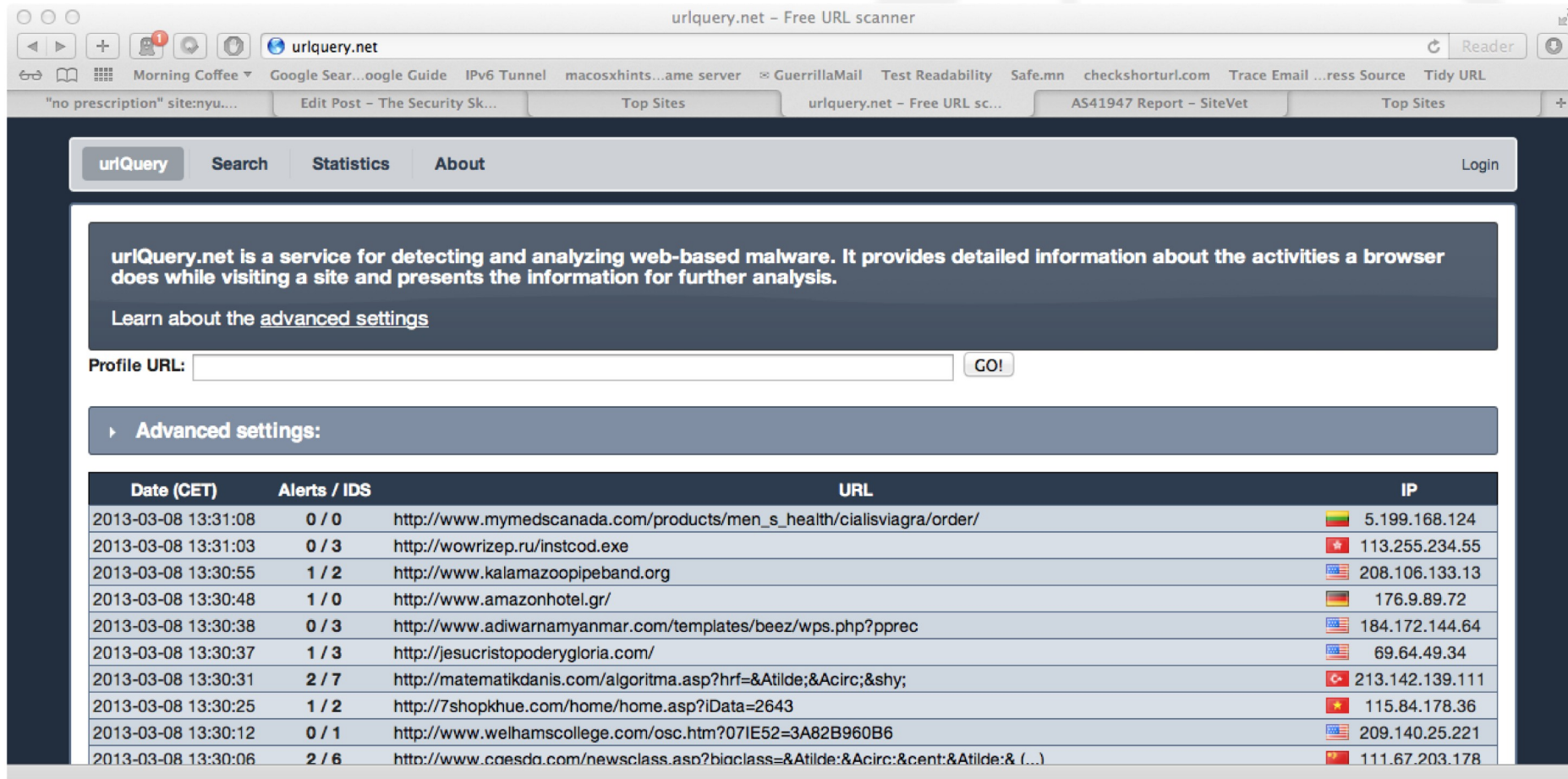
Google

VirusTotal

Reputation Services

- Organizations that classify
 - IP address allocations,
 - Domain names,
 - hosting providers,
 - ISPs,
 - mail operators
- As legitimate or malicious using a scoring system
- URLQuery.net
- sitevet.com
- HOSTexploit.com
- Spamhaus.org
- SenderScore.org
- ProjectHoneypot.org
- MalwareDomainList

Investigate URLs



The screenshot shows the urlquery.net website, which is a free URL scanner. The browser's address bar displays "urlquery.net". The website's navigation bar includes links for "urlQuery", "Search", "Statistics", "About", and "Login". A dark banner at the top explains the service: "urlQuery.net is a service for detecting and analyzing web-based malware. It provides detailed information about the activities a browser does while visiting a site and presents the information for further analysis." Below this banner is a "Profile URL:" input field with a "GO!" button. A section titled "Advanced settings:" is also visible. The main content area displays a table of detected URLs and their associated IP addresses.

Date (CET)	Alerts / IDS	URL	IP
2013-03-08 13:31:08	0 / 0	http://www.mymedscanada.com/products/men_s_health/cialisviagra/order/	5.199.168.124
2013-03-08 13:31:03	0 / 3	http://wowrizep.ru/instcod.exe	113.255.234.55
2013-03-08 13:30:55	1 / 2	http://www.kalamazoopipeband.org	208.106.133.13
2013-03-08 13:30:48	1 / 0	http://www.amazonhotel.gr/	176.9.89.72
2013-03-08 13:30:38	0 / 3	http://www.adwarnamyanmar.com/templates/beeze/wps.php?pprec	184.172.144.64
2013-03-08 13:30:37	1 / 3	http://jesucristopoderygloria.com/	69.64.49.34
2013-03-08 13:30:31	2 / 7	http://matematikdanis.com/algorithm.asp?hrf=ÃÂ­	213.142.139.111
2013-03-08 13:30:25	1 / 2	http://7shopkhue.com/home/home.asp?iData=2643	115.84.178.36
2013-03-08 13:30:12	0 / 1	http://www.welhamcollege.com/osc.htm?07IE52=3A82B960B6	209.140.25.221
2013-03-08 13:30:06	2 / 6	http://www.coesda.com/newsclass.asp?bioclass=ÃÂ¢Ã& (...)	111.67.203.178

http://urlquery.net

Investigate hosts: SITEVET

AS29073 Report - SiteVet

HostExploit

SV AS29073 Report - SiteVet

sitevet.com/db/asn/AS29073

Google

Home Demo Bad Hosts About Us Help Contact Us Members' area

Welcome to SiteVet

SiteVet is in BETA development

Search our database

AS29073

Search

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

AS29073

CURRENTLY ONLINE

HE Index: **152.4**

HE Rank: **1**

Download full report

It's free!

AS Name: ECATEL-AS AS29073, Ecatel Network

IPs allocated: 13056

Blacklisted URLs: 684

Hosts...

- ...malicious URLs? Yes
- ...badware? Yes
- ...botnet C&C servers? Yes
- ...exploit servers? No
- ...Zeus botnet servers? Yes
- ...Current Events? Yes
- ...phishing servers? Yes
- ...spam servers? No
- ...spam bots? Yes

History

Historical Badness

HE Index

Date

2010-07-05 2011-06-23

HE Index

HOSTexploit

Home News Blog Downloads Media Tools Advice

TOP 10 BAD HOSTS - 2013 Q1

HE Rank	HE Index	AS Number	Name
1	152.38	AS29073	Ecatel Network
2	149.22	AS58001	Ideal Solution Ltd
3	146.69	AS6697	Beltelecom
4	141.69	AS29182	ISPsystem
5	136.65	AS16276	OVH Systems
6	134.49	AS24940	Hetzner Online AG
7	133.96	AS40034	Confluence Networks Inc VG
8	133.83	AS197774	Smovskaya Valentina Ivanovna
9	132.18	AS11042	Landis Holdings Inc

<http://hostexploit.com/>

<http://sitevet.com>

MalwareDomainList

- <http://malwaredomainlist.com>

M A L W A R E D O M A I N L I S T

[Homepage](#) | [Forums](#) | [Recent Updates](#) | [RSS update feed](#) | [Contact us](#)


WARNING: All domains on this website should be considered dangerous. If you do not know what you are doing here, it is recommended you leave right away. This website is a resource for security professionals and enthusiasts.

Search: All Results to return: 50 ☐ Include inactive sites

Page [0](#) [1](#) ... [27](#)

Date (UTC)	Domain	IP	Reverse Lookup	Description	Registrant	ASN
u d	u d	u d	u d	u d	u d	u d
2014/07/06_13:07	www.amazonsicherheitonline.com/	151.248.125.133	151-248-125-133.ovz.vps.regruhosting.ru.	Amazon phishing	Registrar Abuse Contact abuse@bizcn.com	39134
2014/06/26_14:27	www.aerreravasi.com	213.205.40.169	web-vip-it.eu.tiscali.it.	iFrame.Exploit	Registrar Abuse Contact abuse@ascio.com	8612
2014/06/26_14:27	www.aerreravasi.com/bolle/bolle.html	213.205.40.169	web-vip-it.eu.tiscali.it.	iFrame.Exploit	Registrar Abuse Contact abuse@ascio.com	8612
	www.aerreravasi.com/		web-vip-it.eu.tiscali.it.		Registrar Abuse Contact	

Domain and URL Block Lists

SPAMHAUS

HomeSBLXBLPBL**DBL**DROPRKSOAbout S

Blocklist Removal Center


DBL Advisory

Blocklist Help

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

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.

SPAMHAUS THE SPAMHAUS PROJECT

HomeSBLXBLPBLDBLDROPRKSOWhitelist

ROKSO Home | ROKSO FAQs & Policies | About Spamhaus | FAQs

Register Of Known Spam Operations


Search ROKSO

ROKSO Documents
► About ROKSO
► ROKSO Listing Policy
► TOP 10 ROKSO Spammers

ROKSO
100 Known Spam Operations responsible for 80% of your spam.
80% of spam received by Internet users in North America and Europe can be traced via aliases, addresses, redirects, locations of servers, domains and dns setups, to a

The ROKSO List

Known Spam Operation	08/23/2012
Country	
7Reach LLC	United States
Abdullah Taeb	United States
Ace Media	United States
Alan Alvarez - DMG	United States
Alejandro Vidal	United States
Alex Blood / Alexander Mosh / AlekseyB / Alex Polyakov	Ukraine
Alex Prihodko / Twinlinks / expo-MAX	Canada
Andrew Stephens / Mail Mascot	United States
Andria Petito / Tranzact Media	United States
Anton Gorodov / Gorodetsk - srx / s-rx	Russian Federation

**SURBL**

URI REPUTATION DATA

HomepageListsLinksNewsMost Abused

SURBL Lists

SURBLs contain web sites that appear in unsolicited messages. check message body web sites against SURBLs, such as SpamAssassin links page.

Here's an overview of the lists and their data sources.

- sc.surbl.org - SpamCop web sites
- ws.surbl.org - sa-blacklist web sites
- ob.surbl.org - Outblaze URI blacklist
- ab.surbl.org - AbuseButler web sites
- ph - Phishing and malware sites
- jp - jwSpamSpy + Prolocation sites
- multi.surbl.org - Combined SURBL list

sc.surbl.org - SpamCop web sites
sc.surbl.org contains message-body web sites processed from S

SenderScore.org

Return Path, Inc. [US] https://senderscore.org/lookup.php?lookup=ntradinginc.com&ip...



Home | About Sender Score | Blacklist Lookup | Fre

Find a Sender Score

Sender Score.org Free Email Reputation from Return Path

Sender Score is Return Path's comprehensive reputation database covering email senders worldwide. [Learn more](#)

Sender Score Metrics for ntradinginc.com

Sending Domain Information

X MX Record [?](#) **X** SSL Certificate
X SPF Record [?](#)

[Whois Lookup](#)

Sending IPs ?	Hostname ?	Authentication ?	Volume ?	Sender Score ?
209.85.217.194	mail-lb0-f194.google.com	Not Authenticated	Very High	58
209.85.217.195	mail-lb0-f195.google.com	Not Authenticated	Very High	52

1 - 2 of 2 [<](#) [>](#)

Related Sending Domains [?](#)

No domains to display.

Latest f

18 Ways
Process

New Sp

New App
with Too

Don't Le
Email P

The Ret
Goes to.

The Ret
Goes to.

Sender Score.org

Free Email Reputation from Return Path

Sender Score is Return Path's comprehensive reputation database covering email senders worldwide. [Learn more](#)

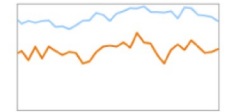
Sender Score Metrics for 209.85.217.194

58

Hostname: mail-lb0-f194.google.com
Very High Volume Sender [?](#)

X Return Path Certified [?](#)
X Return Path Safe [?](#)

[Whois Lookup](#)



Oct 1 Sender Score Volume Oct 31

Recent Campaigns

Subject Line	Date	From Domain	% Inbox	Spam
GET BACK TO ME WITH UPDA...	10/30/13	gmail.com	Contact us for details	
hi	10/28/13	gmail.com	Contact us for details	
We have your cash Consigne...	10/28/13	email.arizona.edu	Contact us for details	

Reputation Measures [?](#)

Impact on this score [?](#)

Blacklists ?	Low
Complaints ?	High
Infrastructure ?	Low
ISP Bulk Rate ?	Contact us for details
Message Filtered ?	High
Sender Rejected ?	Low
Spam Traps ?	15
Unknown Users ?	High

Sending Domains [?](#)

Authentication [?](#)

10dollsrnw.com	SPF - Pass
18digital.com.br	SPF - Pass
24-7contracting.com	SPF - Pass
2pc.com.mx	SPF - Pass
abap-pe.com.br	SPF - Pass
abcnacotinha.com.br	SPF - Pass
accesshdsd.net	SPF - Pass
acicam.com.br	SPF - Pass
acitech.org	SPF - Pass
acslegalcollection.com	SPF - Pass

1 - 10 of 1,430 [<](#) [>](#)

Other IPs with the same hostname [?](#)

ProjectHoneyPot.org

IP Address Inspector

ATTENTION

- This IP has not seen any suspicious activity within the last 3 months. This IP is most likely clean and trustworthy now. (This record will remain public for historical purposes, however.)



Welcome, Dave | [Logout](#)
[Fund the Cause](#) | [Buy Swag](#)
[Refer a Friend](#) | [Terms of Use](#)

[Home](#) [IP Data](#) [Statistics](#) [Services](#) [Help](#) [About](#)
[Directory of IPs](#) [Lookup IP](#) [Harvesters](#) [Spam Servers](#) [Dictionary Attackers](#) [Comment Spammers](#)

Directory of Malicious IPs

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

Global Statistics
Last Bad Event
Any IP
Harvesters
Spam Servers
Bad Web Hosts
Comment Spammers
Dictionary Attackers
Rule Breakers
Search Engines

specific IP address.

The list below is comprised of Malicious IPs (limited to the top 50) that are:

- Arranged by their **Last Bad Event**

Malicious IP	Event	Total	First	Last
161.69.14.152 C	Bad Event	11,307	2013-06-29	2013-10-31
112.123.168.77 C	Bad Event	35,558	2013-01-17	2013-10-31
60.173.10.249 CW	Bad Event	4,039	2010-07-22	2013-10-31
178.137.162.196 SC	Bad Event	14,306	2010-10-21	2013-10-31
112.123.168.156 C	Bad Event	62,817	2013-03-15	2013-10-31
173.44.37.250 HC	Bad Event	949,804	2012-01-23	2013-10-31
208.115.109.114 C	Bad Event	1,511	2012-09-18	2013-10-31
36.248.46.111 C	Bad Event	435	2013-10-29	2013-10-31
60.173.9.60 C	Bad Event			
60.173.10.228 C	Bad Event			

Directory of Dictionary Attacker IPs

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

Global Statistics
Last Bad Event
Dictionary Attackers
From All Countries

See [comment spammers](#), [dictionary attackers](#), or [mail servers](#) from the same region.

The list below is comprised of Dictionary Attacker IPs (limited to the top 50) that are:

- Arranged by their **Last Bad Event**

Dictionary Attacker IP	Event	Total	First	Last
188.143.232.111 SDC	Bad Event	180,331	2011-02-13	2013-10-31
91.207.6.102 SDC	Bad Event	12,786	2013-02-24	2013-10-31
91.124.14.149 SDC	Bad Event	101	2008-01-11	2013-10-31
91.200.13.14 SDC	Bad Event	8,448	2008-12-20	2013-10-31
118.97.80.59 SDC	Bad Event	544	2011-02-26	2013-10-31
186.136.23.189 SD	Bad Event	2,435	2013-08-29	2013-10-31
121.17.125.13 D	Bad Event	495	2013-10-19	2013-10-31
122.142.248.88 SD	Bad Event	62,017	2012-07-17	2013-10-31

119.1.109.41

We don't have data on this IP currently. If you know something, you may [leave a comment](#).

Lookup IP In: [Domain Tools](#) | [SpamHaus](#) | [Spamcop](#) | [SenderBase](#) | [Google Groups](#) | [Google](#)

Geographic Location China

Threat Rating 56 ([Read More](#))

First Bad Host Appearance approximately 3 months, 5 weeks ago

Last Bad Host Appearance within 3 months, 4 weeks

Bad Host Appearances 25,737 appearance(s) in spam e-mail or spam post urls

IPs in The Neighborhood

119.1.109.4 W	
119.1.109.6	
119.1.109.13 W	
119.1.109.15	
119.1.109.16	
119.1.109.17	
119.1.109.28 CR	

Tracking down malware domains

I've got what I think is malware

- How do I figure out if it's a malware?
- How do I figure out if it's controlled via a domain or host?
- Malware analysis methodologies include:
 - Grab a sample: fingerprint files, dissect, disassemble...
 - Run wireshark to capture traffic
 - Catalog the IPs and ASNs of hosts exchanging traffic with my botted machine
 - Passively map DNS
 - Share what I find with other skilled white hats
- Consider using publicly available tools

See *Practical Malware Analysis* by Chris Kendall & Chad McMillan:

http://www.blackhat.com/presentations/bh-dc-07/Kendall_McMillan/Presentation/bh-dc-07-Kendall_McMillan.pdf

Analyzing Malicious Documents

- Locate potentially malicious embedded code, such as shellcode, VBA macros, or JavaScript.
- Execute in a sandbox for analysis.
- Extract suspicious code segments from the file.
- If relevant, disassemble and/or debug shellcode.
- If relevant, deobfuscate and examine JavaScript, ActionScript, or VB macro code.
- Understand next steps in the infection chain.

Tools for analyzing MS Office files

- OfficeMalScanner:
 - locates shellcode, VBA macros in MS Office files
<http://www.reconstrucster.org/code/OfficeMalScanner.zip>
- MalHost-Setup (**Part of OfficeMalScanner**)
 - extracts shellcode from a given offset in an MS Office file and embeds it an EXE file for further analysis. Offvis
 - shows raw contents and structure of an MS Office file, and identifies some common exploits <http://go.microsoft.com/fwlink/?LinkId=158791>
- Hachoir-urwid
 - Navigate structure of binary Office files, view stream contents
<https://bitbucket.org/haypo/hachoir/wiki/hachoir-urwid>

From <http://zeltser.com/reverse-malware/analyzing-malicious-documents.html> - Lenny Zeltser

Tools for analyzing MS Office files

- Office Binary Translator
 - converts DOC, PPT, and XLS files into Open XML files (includes BiffView tool) - <http://b2xtranslator.sourceforge.net/>
- Document Analyzer (<http://documentanalyzer.net>)
 - Launch suspicious office, pdf files in sandbox for inspection, analysis
- FileHex (not free - <http://www.heaventools.com/>) and FileInsight (<http://vil.nai.com/vil/averttools.aspx>)
 - hex editors tp parse and edit OLE structures.
- MalwareTracker PDF examiner
 - <https://www.malwaretracker.com/pdf.php>

From <http://zeltser.com/reverse-malware/analyzing-malicious-documents.html> - Lenny Zeltser

Web-Based Malware analysis

- Upload malware sample or URL
- Various kinds of analyses:
 - Static, Behavioral, Network
 - Composition, dropped files
- virustotal – <http://www.virustotal.com>
- wepawet – <http://wepawet.iseclab.org>
- Anubis – <http://anubis.iseclab.org>
- Malwr - <https://malwr.com>

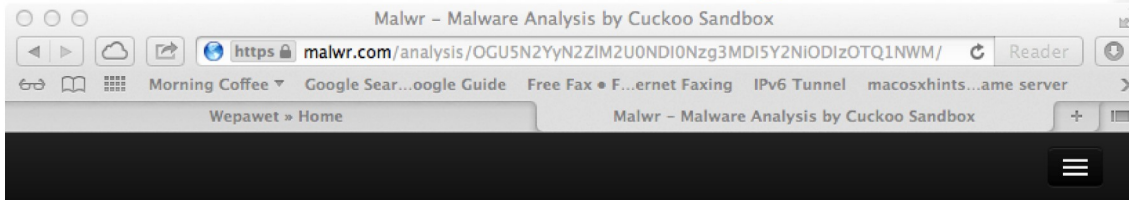
Malware Scanner: Anubis

The image displays the Anubis malware scanner interface. The main window shows an analysis report for 'cobrsa.cpl'. The report includes a table of contents with sections for General Information, dll analysis.exe, and Registry Activities. The 'dll analysis.exe' section is expanded, showing general information about the executable, including its filename, MD5, SHA-1, file size, command line, process status, and exit code. Below this, there are sections for Load-time DLLs, Run-time DLLs, Program output (Stdout), and Stderr. The 'Stdout' section shows the output of the analysis, including the renaming of the input file, finding the entry point, and invoking the 'regsvr32' command. The 'Stderr' section shows the message 'Reloaded Dll bound to different address'.

Overlaid on the main window is a smaller browser window showing the Anubis website. The website has a header with the Anubis logo and navigation links. A large black box with white text is overlaid on the website, displaying the URL: <http://anubis.iseclab.org/index.php>. Below the URL, there is a text box with the following text: 'Submit your Windows executable or Android APK. Alternatively, submit a suspicious URL and receive a report that shows you all the process when visiting this URL.'

http://anubis.iseclab.org/?action=result&task_id=187c4734009b5c574195e1b8c45471e11&format=html

Malware Analysis: malwr



Quick Overview

Static Analysis

Behavioral Analysis

Network Analysis

Dropped Files

Comment Board (1)

Flattr this!

Tags: **Phishing** **Phishing Attachment**

Analysis

CATEGORY	STARTED	COMPLETED	DURATION
FILE	2013-06-21 09:16:50	2013-06-21 09:19:05	135 seconds

File Details

FILE NAME	LexisNexis_Invoice_06212013.exe
FILE SIZE	116736 bytes
FILE TYPE	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
MD5	59b6b3a45afd6fad05977f923cc12e15
SHA1	7a1f6bec3bc04ca7c48516b5f806fb39d3cb1530



Quick Overview

Static Analysis

Behavioral Analysis

Network Analysis

Dropped Files

Comment Board (1)

Domains (8) Hosts (41) HTTP (17) IRC (0) SMTP (0)

Domains

DOMAIN	IP
coolstowage.com	174.140.168.239
www.finanze.konzepte-czekalla.de	82.165.48.194
fallimentodipietrosipa.it	62.149.223.223
www.google.com	173.194.66.106
www.google.nl	173.194.66.94
gpbit.com	5.9.83.152
cdn162.filesbest4upload.com	78.131.140.151
keep-smile.net	184.154.165.50



Quick Overview

Static Analysis

Behavioral Analysis

Network Analysis

Dropped Files

Comment Board (1)

Domains (8) Hosts (41) **HTTP (17)** IRC (0) SMTP (0)

HTTP Requests

URI	DATA
http://coolstowage.com/ponyb/gate.php	POST /ponyb/gate.php HTTP/1.0 Host: coolstowage.com Accept: */* Accept-Encoding: identity, *,q=0 Accept-Language: en-US Content-Length: 271 Content-Type: application/octet-stream Connection: close Content-Encoding: binary User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2)

<https://malwr.com>

Memory Scanners and Analyzers

The screenshot shows the ThreatExpert website interface. The 'Memory Scanner' link is highlighted with a red circle. The website includes a navigation bar with links like Home, ThreatExpert Reports, Tools, Threat Browser, Submit Sample, and About ThreatExpert. The main content area features a 'Welcome to ThreatExpert' message, a list of malware samples, a 'Geographic Distribution of' map, and a 'Memory Scanner' section with a 'Scan your PC for threats' button. The 'Memory Scanner' section is circled in red.

ThreatExpert – Automated Threat Analysis

Home ThreatExpert Reports Tools Threat Browser Submit Sample About ThreatExpert

Welcome to ThreatExpert

ThreatExpert is an advanced automated threat analysis system designed to analyze and report the behavior of malware, spyware, and other security-related risks in a fully automated mode.

In only a few minutes ThreatExpert can process a sample and generate a highly detailed threat report with the level of detail that exceeds antivirus industry standards such as those normally found in online virus encyclopedias.

[Learn More](#)

Malware Adware

Trojan.Lineage.Gen!Pac.3

Trojan.Popuper

Worm.IM.Sohanad

Application.Ardamax_Keylogger

Email-Worm.Brontok

Win32.Virut.Gen.5

RogueAntiSpyware.AntiVirusPro

Worm.Hamweg.Gen

Win32.Sality.AM.Gen

Rootkit.Podnuha.Gen.2

Geographic Distribution of

China

Russian Federation

Brazil

United Kingdom

United States

Spain

Germany

United States

Spain

Germany

Russian Federation

To see the World Threat Atlas please [Follow here](#)

Submission Applet

Submit samples from your desktop

Memory Scanner

Scan your PC for threats

ThreatFire

Behavioral AntiVirus - Protect your PC from threats

ThreatExpert Blog

A Blog about an automated threat analysis

Latest Reported Threats

Find: php

Next Previous Highlight all Match case Reached end of page, continued from top

Desktop tools at Mandiant Community Software:
<http://www.mandiant.com/resources/downloads>

Investigating web sites or pages

- You may not want to visit a suspicious site using a browser
- If you want to see HTTP responses but don't trust to *execute* use
 - cURL
 - <http://curl.haxx.se/docs/manpage.html>
 - <http://www.thegeekstuff.com/2012/04/curl-examples/>
 - Want to curl Gmail for new email? `curl -u username --silent "https://mail.google.com/mail/feed/atom" | perl -ne 'print "\t" if /<name>/; print "$2\n" if /<(title|name)>(.*?)<\1>/;'`
 - Wget
 - <http://www.gnu.org/software/wget/>
 - <http://gnuwin32.sourceforge.net/packages/wget.htm>
 - Capture traffic with LAN traffic analyzers (wireshark)
- Want to see a site that's no longer online?
 - try Wayback Machine at <http://archive.org>

Investigating web pages

```
○ ○ ○ davepiscitello — bash — 80×44
Daves-MacBook-Pro:~ davepiscitello$ curl -v http://www.internic.net
* About to connect() to www.internic.net port 80 (#0)
*   Trying 192.0.32.9...
* connected
* Connected to www.internic.net (192.0.32.9) port 80 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.24.0 (x86_64-apple-darwin12.0) libcurl/7.24.0 OpenSSL/0.9.8
r zlib/1.2.5
> Host: www.internic.net
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Fri, 24 Aug 2012 00:04:20 GMT
< Server: Apache
< Last-Modified: Wed, 05 Oct 2011 20:54:31 GMT
< ETag: "45a3f-1c94-4ae936a23cfc0"
< Accept-Ranges: bytes
< Content-Length: 7316
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<head>
<title>InterNIC | The Internet's Network Information Center</title>
<meta content="text/html; charset=utf-8" http-equiv=Content-Type>
<meta name="keywords"
      content="internic,network information, domain registration">
```

cURL supports DICT, FILE,
FTP, FTPS, Gopher, HTTP,
HTTPS, IMAP, IMAPS, LDAP,
LDAPS, POP3, POP3S,
RTMP, RTSP, SCP, SFTP,
SMTP, SMTPS, Telnet, TFTP

Investigating hosts

```
dave — bash — 70x15
Last login: Tue Jan 15 08:22:05 on ttys000
Davids-MacBook-Air-2:~ dave$ dig www.datestars-girls.ru
; <<>> DiG 9.7.6-P1 <<>> www.datestars-girls.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57427
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.datestars-girls.ru.      IN      A

;; ANSWER SECTION:
www.datestars-girls.ru. 21600  IN      A      84.22.127.98
```

1 site hosted on IP Address 84.22.127.98

Same IP

ID	Domain	Site Link
1	bridesko.ru	bridesko.ru

Updated at 2013-01-15 09:46:42

Copyright © Find All Website On The Same IP Address - Contact Us - Privacy Policy
Daily Domain Spv | Daily Domains | Name Server Spv

Find all domains hosted on the same IP address

sameip.org

Reverse IP Lookup

84.22.127.98

Ex: google.com, yahoo.com, 94.107.252.10

- [sites hosted on IP Address 210.15.218.90](http://sameip.org/ip/210.15.218.90)
...
<http://sameip.org/ip/210.15.218.90> - 2013-01-15 08:58
- [sites hosted on IP Address 210.15.218.53](http://sameip.org/ip/210.15.218.53)
...
<http://sameip.org/ip/210.15.218.53> - 2013-01-15 08:57

You identify
a spam domain

What other
domains
are hosted
at this IP?

And... more Russian brides!

Advanced search operators

"no prescription" site:edu - Google Search

Looking For Arimidex (Cheap Arimidex **No Prescription**)? Buy Arimidex Here. Cheapest Arimidex Prices, Fast Worldwide Shipping, **No Prescription** Required.

[Desyrel **No Prescription**. Cheapest Desyrel Prices Guaranteed ...](#)
[comm.louisville.edu/abi/wp-sto/pills/?pill...no-prescription](#)
Looking For Desyrel (Desyrel **No Prescription**)? Buy Desyrel Here. Cheapest Prices, Fast Worldwide Shipping, **No Prescription** Required. Order Desyrel ...

[Buy Mobic **No Prescription**. Cheapest Mobic Prices Guaranteed ...](#)
[comm.louisville.edu/abi/wp-sto/pills/?pill...no-prescription](#)
Looking For Mobic (Buy Mobic **No Prescription**)? Buy Mobic Here. Cheapest Mobic Prices, Fast Worldwide Shipping, **No Prescription** Required. Order Mobic ...

[Viagra Brand Online, Order Viagra **No Prescription** - Pill Shop ...](#)
[www.tsbvi.edu/resources/3318-onhsod-survey](#)
Viagra Brand Online, Order Viagra **No Prescription**. Brand viagra online usa without prescription mail order no genuine original cheap cheapest. Order cheap ...

[Cheap **No Prescription** Cialis, Canada Cialis - Canadian Pharmacy ...](#)
[ace.nd.edu/advocates/regions/new-orleans](#)
Prescription requirements canada cialis generic cheap acheter du générique cheap **no prescription** cialis au super ontario online pills without no free shipping ...

< **Go**oooooooooooo **gle** >

[Previous](#) 1 2 3 4 5 6 7 8 9 10 [Next](#)

[Advanced search](#) [Search Help](#) [Give us feedback](#)

[Google Home](#) [Advertising Programs](#) [Business Solutions](#) [Privacy & Terms](#)

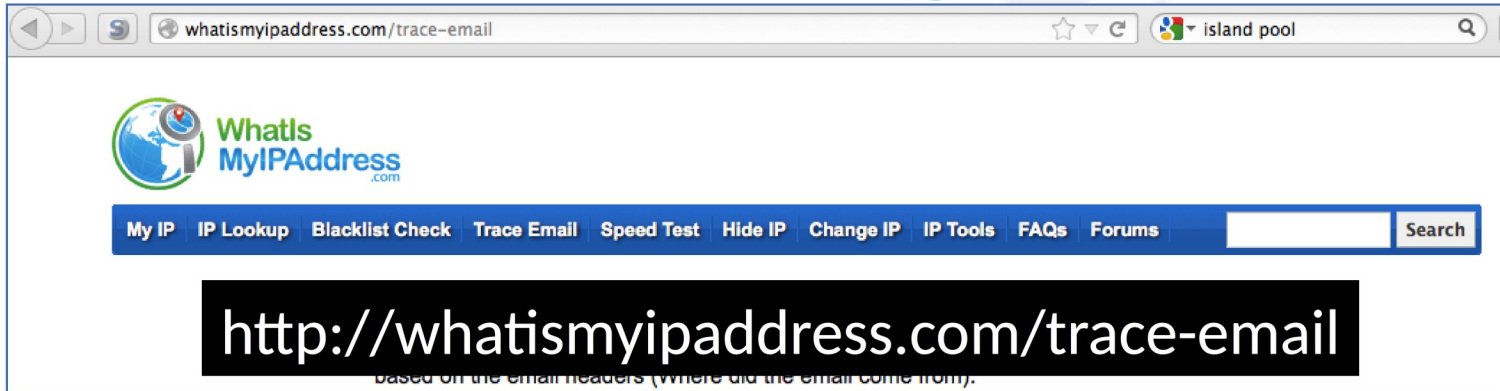
Find hacked University Wordpress sites

Also try the string "Powered by Wordpress"

The WOT extension previews page

http://www.googleguide.com/advanced_operators.html

Tools for Examining Mail Headers



Headers:

```
Received: from ppa3.lax.icann.org (192.0.33.78) by EXPFE100-1.exc.icann.org
(64.78.22.245) with Microsoft SMTP Server (TLS) id 8.3.245.1; Thu, 23 Aug
2012 08:32:35 -0700
Received: from pectoral.lax.icann.org (pectoral.icann.org [192.0.33.71])
by
  ppa3.lax.icann.org (8.14.4/8.14.4) with ESMTP id q7NFWYQ9003907
  (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=NOT)
for
  <dave.piscitello@ppa-ex.icann.org>; Thu, 23 Aug 2012 16:32:34 +0100
Received: from ppal.lax.icann.org (ppal.lax.icann.org [192.0.33.76]) by
  pectoral.lax.icann.org (8.13.8/8.13.8) with ESMTP id q7NFWXj8019514
  <dave.piscitello@icann.org>; Thu, 23 Aug 2012 15:32:34 GMT
Received: from pps.reinject (ppal [127.0.0.1]) by ppal.lax.icann.org
(8.14.4/8.14.4) with ESMTP id q7NFVVA1011229 (version=TLSv1/SSLv3
  cipher=DHE-RSA-AES256-SHA bits=256 verify=NOT) for
  <dave.piscitello@icann.org>; Thu, 23 Aug 2012 16:31:33 +0100
Received: from pps.reinject (ppal [127.0.0.1]) by pps.reinject (8.14.4/8.14.1)
  with SMTP id q7NFVVq6011221 for <dave.piscitello@icann.org>; Thu, 23 Aug
  2012
  16:31:31 +0100
Received: from pectora5.dc.icann.org (pectora5.icann.org [192.0.46.71]) by
```

[Get Source](#)

Copy-past raw headers

Analysis:

```
Received: from ppa3.lax.icann.org (192.0.33.78) by EXPFE100-1.exc.icann.org (64.78.22.245) with Microsoft SMTP Server (TLS)
id 8.3.245.1; Thu, 23 Aug 2012 08:32:35 -0700
Received: from pectora1.lax.icann.org (pectora1.icann.org [192.0.33.71]) by ppa3.lax.icann.org (8.14.4/8.14.4) with ESMTP id
q7NFWYQ9003907 (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=NOT) for <dave.piscitello@ppa-
ex.icann.org>; Thu, 23 Aug 2012 16:32:34 +0100
Received: from ppa1.lax.icann.org (ppa1.lax.icann.org [192.0.33.76]) by pectora1.lax.icann.org (8.13.8/8.13.8) with ESMTP id
q7NFWXj8019514 for <dave.piscitello@icann.org>; Thu, 23 Aug 2012 15:32:34 GMT
Received: from pps.reinject (ppa1 [127.0.0.1]) by ppa1.lax.icann.org (8.14.4/8.14.4) with ESMTP id q7NFVVA1011229
(version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=NOT) for <dave.piscitello@icann.org>; Thu, 23 Aug 2012
16:31:33 +0100
Received: from pps.reinject (ppa1 [127.0.0.1]) by pps.reinject (8.14.4/8.14.1) with SMTP id q7NFVVq6011221 for
<dave.piscitello@icann.org>; Thu, 23 Aug 2012 16:31:31 +0100
Received: from pectora5.dc.icann.org (pectora5.icann.org [192.0.46.71]) by ppa4.dc.icann.org with ESMTP id q7BMSgbN018126
(version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=NOT) for <dave.piscitello@ppa-ex.icann.org>; Sat, 11 Aug
2012 23:28:42 +0100
Received: from wsu-ironport01-outbound.merit.edu (wsu-ironport01-outbound.merit.edu [141.217.151.138]) by
  pectora5.dc.icann.org (8.13.8/8.13.8) with ESMTP id q7BMSKK1022749 for <ssac-fellow@icann.org>; Sat, 11 Aug 2012 22:28:42
  GMT
Received: from 96-32-68-10.dhcp.gwnt.ga.charter.com (HELO Unknown) ([96.32.68.10]) by connect.wayne.edu with ESMTP/TLS
/DHE-RSA-AES256-SHA; 11 Aug 2012 18:27:56 -0400
From: TSB Bank <customerservice@tsb.co.nz>
Content-Class: urn:mbox:mail:141217151138
Date: Sat, 11 Aug 2012 18:27:56 -0400
Subject: Important
```

Outputs mail relay path

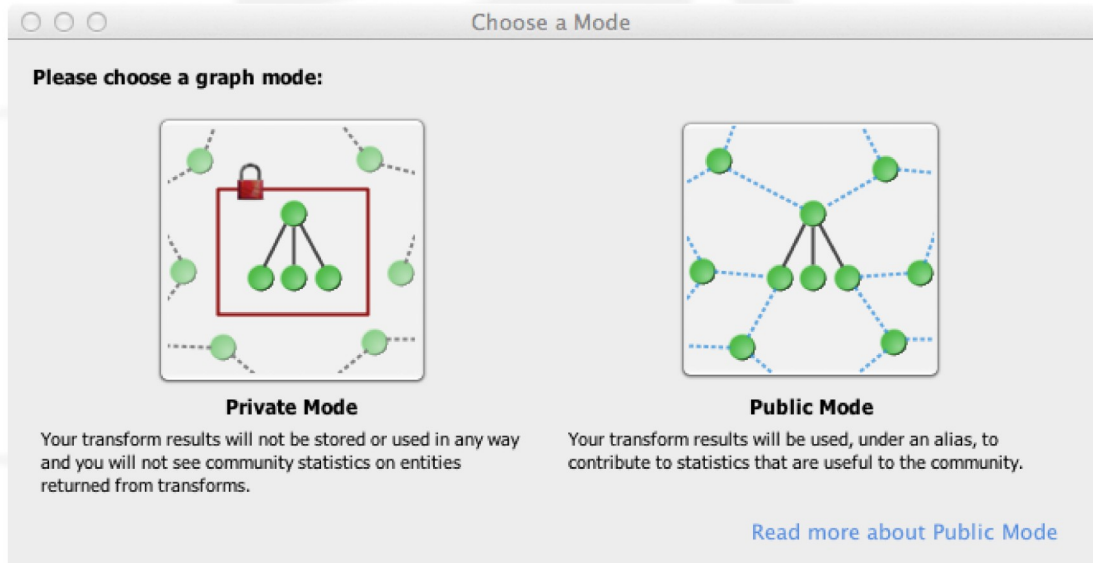


Anonymizers and proxies

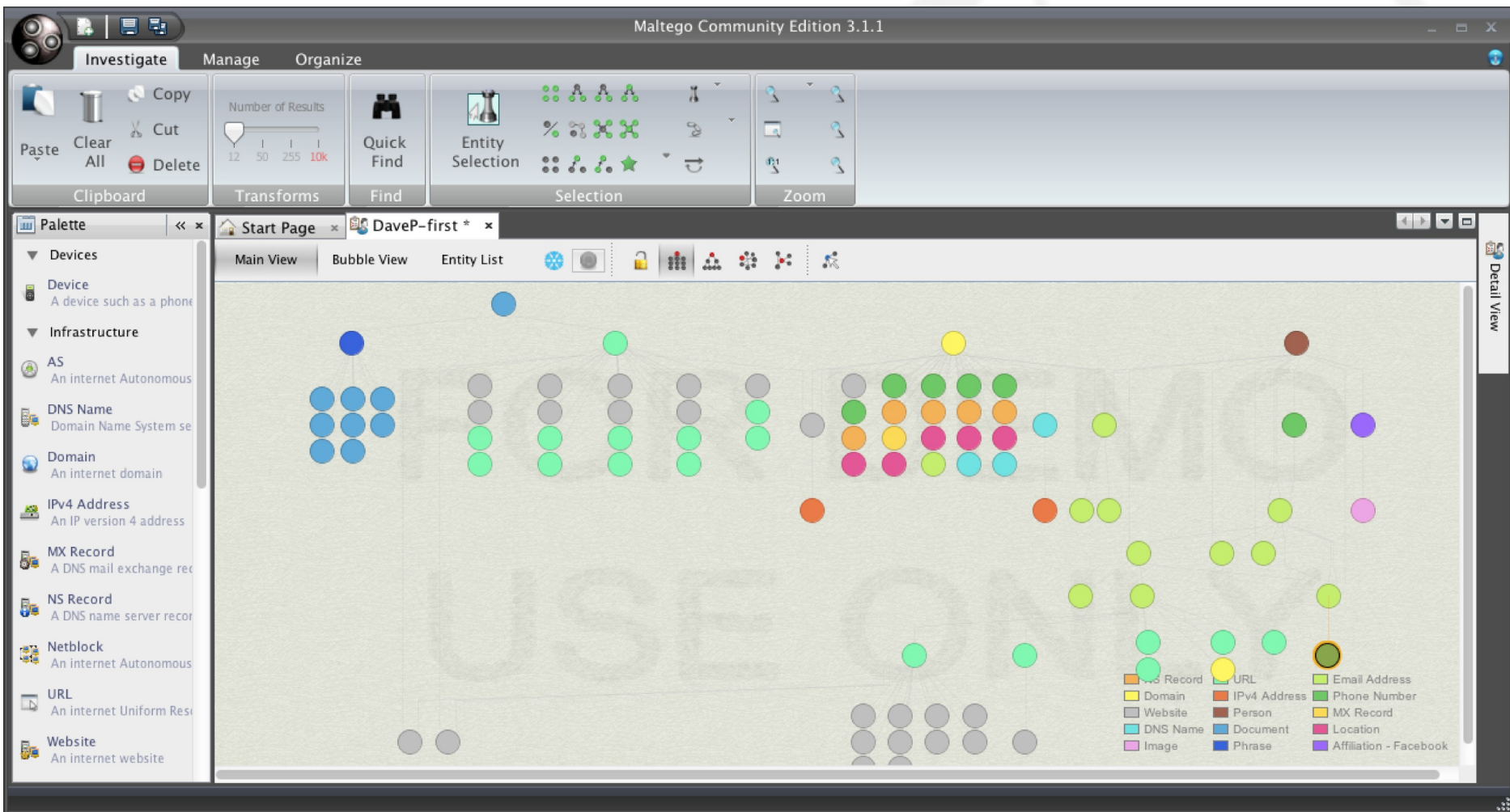
- Bad guys are getting smarter
 - Block IPs of known investigators
 - One-time use for IPs/URLs
- Turn to tools used by them as well
 - TOR <https://www.torproject.org/>
 - Hidemyass <http://hidemyass.com/>
 - Browser add-ons for proxies (random, pick location/country)
 - User agent changes (can do with cURL as well)

Maltego

- Open source *Threat Picture* platform
 - Good for intel gathering or forensics
 - Good way to visualize relationships and associate data you collect from diverse resources
- Client-to-Cloud



Visualize Relationships

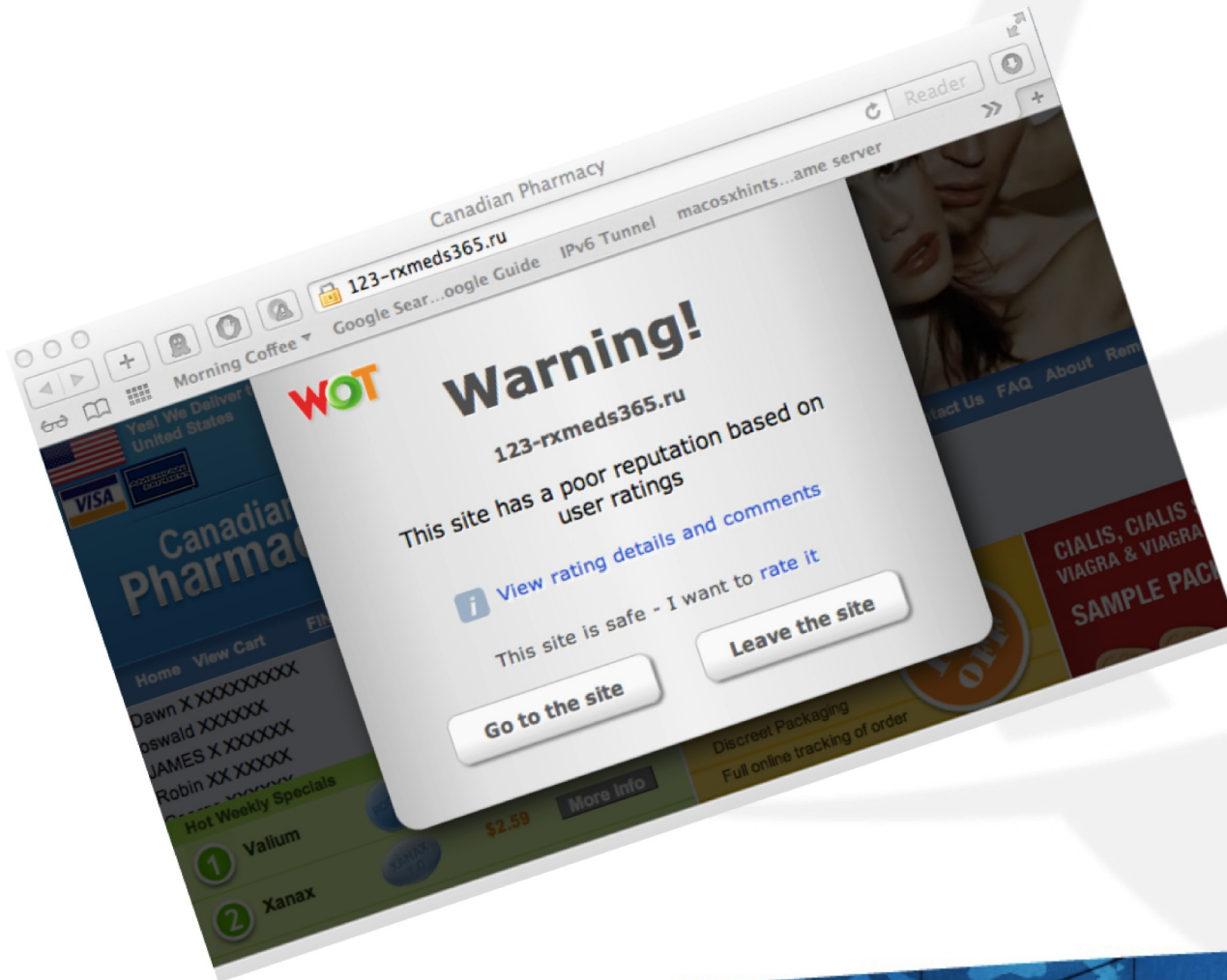


Identify relationships: People, Groups, Social networks, Companies, Organizations, Web sites, Domains, DNS names, Netblocks, IP addresses, Phrases. Affiliations, Documents, Files - *Extensible for your data*

Gathering Intel: Illegal Pharma

A search on
“No prescription”
leads us here.

What can we use
to confirm that
123-rxmeds365.ru
is a malicious
domain?



Dig the domain name

```
% dig 123-rxmeds365.ru
;; QUESTION SECTION:
;123-rxmeds365.ru.
```

“Red flag” TLD,
“Pharma” label
Check Whois?

```
;; ANSWER SECTION:
```

```
123-rxmeds365.ru. 300 IN A 129.7.240.229
123-rxmeds365.ru. 300 IN A 198.61.167.175
123-rxmeds365.ru. 300 IN A 173.248.130.201
123-rxmeds365.ru. 300 IN A 173.230.229.219
```

Dig SOA record?

```
;; AUTHORITY SECTION:
```

```
123-rxmeds365.ru.345598 IN NS ns4.bestrxfast365.ru.
123-rxmeds365.ru.345598 IN NS ns1.directrx724.com.
123-rxmeds365.ru.345598 IN NS ns2.toprxbest.com.
123-rxmeds365.ru.345598 IN NS ns3.myfavoriterx724.ru.
```

```
;; ADDITIONAL SECTION:
```

```
ns4.bestrxfast365.ru.345598 IN A 108.170.47.235
ns2.toprxbest.com. 172798 IN A 63.143.54.116
ns3.myfavoriterx724.ru. 345598 IN A 68.73.80.135
ns1.directrx724.com. 172798 IN A 64.31.37.232
```

Short TTLs
In A records
(fast flux?)

Even Incomplete Whois Tells You Something

[whois.ripn.net]

domain: 123-RXMEDS365.RU
nserver: ns1.directrx724.com.
nserver: ns2.toprxbest.com.
nserver: ns3.myfavoriterx724.ru.
nserver: ns4.bestrxfast365.ru.
state: REGISTERED, DELEGATED, UNVERIFIED
person: Private Person
registrar: NAUNET-REG-RIPN
admin-contact: <https://client.naunet.ru/c/whoiscontact>
created: 2012.02.19
paid-till: 2013.02.19
free-date: 2013.03.22
source: TCI

What raises suspicion?

- Private registration?
- Registry reputation?
- Registrar reputation?
- Creation date (How recent?)
- Name servers?

IP-Whois the Addresses

```
% dig 123-rxmeds365.ru
```

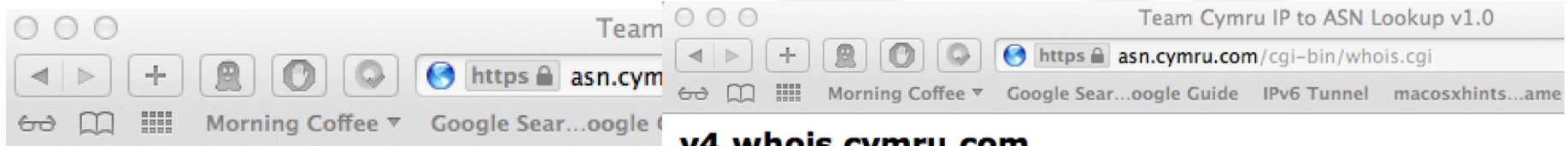
```
;; QUESTION SECTION:
```

```
;123-rxmeds365.ru.          IN      A
```

```
;; ANSWER SECTION:
```

```
123-rxmeds365.ru.  300    IN      A      129.7.240.229
123-rxmeds365.ru.  300    IN      A      198.61.167.175
123-rxmeds365.ru.  300    IN      A      173.248.130.201
123-rxmeds365.ru.  300    IN      A      173.230.229.219
```

Domain is
hosted on 4
different IPs in 4
different ASNs



v4.whois.cymru.com

The server returned 4 line(s).

```
[Querying v4.whois.cymru.com]
[v4.whois.cymru.com]
```

AS	IP	AS Name
7276	129.7.240.229	UNIVERSITY-OF-HOUSTON - Univers

v4.whois.cymru.com

The server returned 4 line(s).

```
[Querying v4.whois.cymru.com]
[v4.whois.cymru.com]
```

AS	IP	AS Name
19994	198.61.167.175	RACKSPACE - Rackspace Hosting

Other IPs are in Softsys Hosting, Baroda India via WeHostWebSites and Globalweb Outsourcing Corp, Aventura FL via

What about the name servers?

```
% dig 123-rxmeds365.ru
;; QUESTION SECTION:
;123-rxmeds365.ru.          IN      A

;; AUTHORITY SECTION:
123-rxmeds365.ru.345598    IN      NS      ns4.bestrxfast365.ru.
123-rxmeds365.ru.345598    IN      NS      ns1.directrx724.com.
123-rxmeds365.ru.345598    IN      NS      ns2.toprxbest.com.
123-rxmeds365.ru.345598    IN      NS      ns3.myfavoriterx724.ru.
```

Name service is

- hosted at four different domains
- Name server IPs are in four different ASNs

Need more intel?

- Whois the name server domains
- Check out the neighborhoods
 - Passive DNS the name servers
 - Look at reputations of hosting providers, ISPs
 - cURL the page for additional domains in hyperlinks

Investigating Malware: Trojan



What else can we find out here?

Quick Overview

File has been identified by at least one AntiVirus on VirusTotal as malicious

Performs some HTTP requests

Unconventional binary language: Russian

Steals private information from local Internet browsers

Harvests credentials from local FTP client softwares

Installs itself for autorun at Windows startup

Screenshots



password stealing
trojan, rootkit

Quick Overview

Static Analysis

Behavioral Analysis

Network Analysis

Dropped Files

Comment Board (0)

Static Analysis

Strings

Antivirus

ANTIVIRUS	SIGNATURE
MicroWorld-eScan	Gen:Varia...mi.25961
nProtect	Clean
CAT-QuickHeal	Clean
McAfee	Clean
Malwarebytes	Spyware.Zbot.ED

Quick Overview

Static Analysis

Behavioral Analysis

Network Analysis

Dropped Files

Comment Board (0)

Quick Overview

Static Analysis

Behavioral Analysis

Network Analysis

Dropped Files

Comment Board (0)

Domains (3)

Hosts (2)

HTTP (13)

IRC (0)

SMTP (0)

Domains

DOMAIN	IP
windowsupdate.microsoft.com	65.55.184.25
tiredclinker.biz	91.220.131.179
pensnuqqetsized.biz	91.220.131.179

Domains (3)

Hosts (2)

HTTP (13)

IRC (0)

SMTP (0)

Hosts

IP
65.55.184.25
91.220.131.179

Next steps?

Next steps?

Get name server info?

```
; <<>> DiG 9.8.3-P1 <<>> NS tiredclinker.biz
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59704
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;tiredclinker.biz.                IN      NS

;; ANSWER SECTION:
tiredclinker.biz.                600     IN      NS      ns2.teamspanama.com.
tiredclinker.biz.                600     IN      NS      ns1.teamspanama.com.
```

What other information
can you gather?

How?

Report to whom?

Passive DNS of name server

Query:

Additional data may be available with this query: [teamspanama.com](#)

The server returned the following data:

teamspanama.com	NS	ns2.teamspanama.com
ns2.teamspanama.com	A	46.37.165.104
audiobookscomputersa.biz	NS	ns2.teamspanama.com
chappellestouched.biz	NS	ns2.teamspanama.com
smartphoneserviceoriented.biz	NS	ns2.teamspanama.com
pensnuggetized.biz	NS	ns2.teamspanama.com
viagraand.biz	NS	ns2.teamspanama.com
fatcompliance.biz	NS	ns2.teamspanama.com
greatsimple.biz	NS	ns2.teamspanama.com
shortercontribute.biz	NS	ns2.teamspanama.com
payablesnf.biz	NS	ns2.teamspanama.com
dnscraking.biz	NS	ns2.teamspanama.com
personefiling.biz	NS	ns2.teamspanama.com
peoplesofttimesaving.biz	NS	ns2.teamspanama.com
casualtiesasterisk.biz	NS	ns2.teamspanama.com
workshopofficial.biz	NS	ns2.teamspanama.com
wlansrelational.biz	NS	ns2.teamspanama.com
forwardshospital.biz	NS	ns2.teamspanama.com
customizesabl.biz	NS	ns2.teamspanama.com
primeguardian.biz	NS	ns2.teamspanama.com
hyperbowlvip.biz	NS	ns2.teamspanama.com
explorationfollowup.biz	NS	ns2.teamspanama.com
beastfollowup.biz	NS	ns2.teamspanama.com
openearedbarcodes.biz	NS	ns2.teamspanama.com
handbagtechnologies.biz	NS	ns2.teamspanama.com
subscribertomatoes.biz	NS	ns2.teamspanama.com
oneofakindmediastudios.biz	NS	ns2.teamspanama.com
clusteringpaperless.biz	NS	ns2.teamspanama.com
barelyalerts.biz	NS	ns2.teamspanama.com
jeffreyearit.biz	NS	ns2.teamspanama.com

Tracking Down a Spam E-mail

From: Claire Newell anarchdd@yeonil.net

Subject: Fwd:

Date: April 4, 2011 5:44:06 PM PDT



Viagra Our price: **\$1.29**
Viagra is an oral drug for male impotence, also known as erectile dysfunction. Viagra has a great safety track record and proven effects that start acting in 30 minutes to 1 hour and last for about 4 hours.

Female Viagra Our price: **\$2.36**
Female Viagra (Sildenafil) is scientifically formulated to provide intense sexual satisfaction for women seeking ultimate pleasure.

Cialis Our price: **\$1.58**
Cialis (Tadalafil) is used for treating erectile men's erectile dysfunction (e.g., impotence). Cialis starts working in 30 minutes and lasts for about 36 hours, while Viagra effect lasts up to 5 hours. Besides, you can take Cialis with or without food.

Levitra Our price: **\$2.81**
Levitra (Vardenafil) is an oral therapy for the treatment of erectile dysfunction. Having the long-lasting effect of 4 hours, and the start time of 16 min, Levitra represents an uncontested advantage in comparison with Viagra.

www.pillsgy.com

Let's
the
hyperlink

What do we find at pillzgy.com

Pharmacy Express
#1 ONLINE WORLDWIDE DRUGSTORE

We ship worldwide USD EUR CAD **GBP** CHF AUD JPY BRL MXN NZD 🛒 Your cart: **GBP 0.00** (0 items)
+1-800 642-1061 🇺🇸 🇩🇪 🇫🇷 🇮🇹 🇪🇸 🇬🇷 🇯🇵

Free Delivery Insurance
7 years WorldWide Supplier
100% Satisfaction Guarantee
High Quality medicaments
24/7/365 Support Team

Main About us F.A.Q. Our policies Track my order Your cart Contact us

Search...

Browse by:

Letter
A B C D E F G H I J K L M N
O P Q R S T U V W X Y Z

Category

- ED Packs **SALE -15%**
- Herbal ★
- Most Popular ★
- Allergy
- Anthelmintics
- Anti Bacterial
- Anti Convulsants
- Anti Depressants

New! The best and cheapest herbal pills
Herbal medications are absolutely safe and high-quality. Without any doubts you can buy Herbal products and your health problems will be solved in the right way! Herbal pills consist of 100 % natural ingredients. So, you won't be bothered by unpleasant side effects. If you decided to buy any Herbal medications we sure you won't be disappointed with its splendid and quickest results.

100% NATURAL

Light Pack | Save 15%
Viagra 50mg x 30
Cialis 10mg x 30
GBP 113.75 **GBP 103.41**
Select pack 🛒

Professional Pack | Save 15%
Viagra Professional 100mg x 30
Cialis Professional 20mg x 30
GBP 192.72 **GBP 175.20**
Select pack 🛒

Viagra Pack | Save 15%
Viagra 100mg x 20
Viagra Professional 100mg x 20
Viagra Super Active 100mg x 20
GBP 155.35 **GBP 141.23**
Select pack 🛒

Generic Viagra
special price: **GBP 0.71**

Generic Cialis
special price: **GBP 0.88**

Most Popular (per pill)
Stro...

What we see if
we open cURL
output
(offline?)

Whois pillsgy.com???


Domain Name: PILLSGY.COM
Registrar: IPNIC, INC.
Whois Server: whois.myorderbox.com
Referral URL: http://www.ipnic.com
Name Server: NS1.DNSPLAC.COM
Name Server: NS2.BEZZDNS.RU
Status: clientTransferProhibited
Updated Date: 03-apr-2011
Creation Date: 18-mar-2011
Expiration Date: 18-mar-2012

Registrant:
Koshil Igor
Igor (KoshilIgor@mail.com)
Koneva str. 12-48
Koneva str. 12-48
Omsk
Omsk, 644031
RU
Tel. +7.3812447211
Fax. +7.3812447211

Creation Date: 18-Mar-2011
Expiration Date: 18-Mar-2012

Domain servers in listed order:
ns1.dnsplac.com
ns2.bezzdns.ru

Administrative Contact:
Koshil Igor
Igor (KoshilIgor@mail.com)
Koneva str. 12-48
Koneva str. 12-48
Omsk
Omsk, 644031
RU
Tel. +7.3812447211
Fax. +7.3812447211



Would
Maltego be
helpful here?

Passive DNS Doesn't Look "Bad"

IP search:

Found 2 records

Host/Domain Name	pillsgy.com
First Seen	2011-03-25 02:43:30
IP	122.224.6.32
ASN BGP	4134
Netblock	122.224.0.0/12
pillsgy.com	2011-03-20 02:28:22 127.0.0.1

Take a closer
look at this IP
address block?

Nameserver search:

Found 4 records

Nameserver	First Seen
ns2.bezzdns.ru	2011-03-25 02:43:27
ns1.dnskt.com	2011-03-25 02:43:27
ns1.ezydomain.com	2011-03-20 02:28:22
ns2.ezydomain.com	2011-03-20 02:28:22

Gather Intel on that IP

inetnum: 122.224.6.0 - 122.224.6.255
netname: NINBO-LANZHONG-LTD
country: CN
descr: Ninbo Lanzhong Network Ltd
descr:
admin-c: TD209-AP
tech-c: CS64-AP
status: ASSIGNED NON-PORTABLE
changed: auto-dbm@dcb.hz.zj.cn 20100105
mnt-by: MAINT-CN-CHINANET-ZJ-SX
source: APNIC

role: CHINANET-ZJ Shaoxing
address: No.9 Sima Road,Shaoxing,Zhejiang.312000
country: CN
phone: +86-575-5136199
fax-no: +86-575-5114449
e-mail: anti-spam@mail.sxptt.zj.cn
trouble: send spam reports to anti-spam@mail.sxptt.zj.cn
Trouble:and abuse reports to anti-spam@mail.sxptt.zj.cn

admin-c: CH109-AP
tech-c: CH109-AP
nic-hdl: CS64-AP
mnt-by: MAINT-CHINANET-ZJ
Changed: master@dcb.hz.zj.cn 20031204
source: APNIC

person: Taichun Du
nic-hdl: TD209-AP
e-mail: anti-spam@mail.sxptt.zj.cn
address: Shaoxing,Zhejiang.Postcode:312000
phone: +86-574-88311333
country: CN
changed: auto-dbm@dcb.hz.zj.cn 20100105
mnt-by: MAINT-CN-CHINANET-ZJ-SX
Source: APNIC

How About a Nameserver?

Passive DNS replication

Found 26 records

First Seen Domain

4/4/2011 1:51	bljxpills.ru
4/3/2011 23:12	brjxpills.ru
4/4/2011 13:51	caxrpills.com
4/3/2011 16:09	chxrpills.com
4/3/2011 16:33	dnsplac.com
4/3/2011 21:45	doctorje.com
4/4/2011 15:47	doctorod.com
4/3/2011 16:20	doctorrg.com
4/3/2011 16:25	doctorrl.com
4/3/2011 23:41	fajxpills.ru
4/4/2011 18:58	gejxpills.ru
4/4/2011 9:32	medicaqap.ru
4/4/2011 8:01	medicaqar.ru

First Seen Domain

4/4/2011 17:02	medicaqch.ru
4/4/2011 10:14	medicaqci.ru
4/3/2011 22:15	medicaqee.ru
4/3/2011 22:18	medicaqen.ru
4/3/2011 22:18	midiclxia.ru
4/3/2011 22:38	midiclxic.ru
4/3/2011 22:46	midiclxme.ru
4/3/2011 22:15	midiclxnf.ru
4/3/2011 22:51	midiclxto.ru
4/4/2011 20:23	pillsin.com
4/3/2011 16:26	pillsl1.com
4/4/2011 23:56	rafpills.com
4/3/2011 21:19	stpills.com

Illegal pharma haven

Your query returned **438,394** records.

First Seen	Host/Domain
3/23/2011 8:59	0.2k.medicsy.com
3/23/2011 10:30	0.2l60.medicsy.com
3/23/2011 21:19	0.3.medicdm.com
3/23/2011 22:42	0.3.medicsy.com
4/4/2011 16:53	0.3.topmedicb.ru
4/4/2011 20:18	0.348t.medicsy.com
3/21/2011 0:00	0.6fj0.medicsy.com
1/27/2011 18:26	0.bsirr.doctorgco.ru
1/26/2011 15:42	0.bsirr.sodoctorg.ru
1/27/2011 8:44	0.bsirr.sudoctorg.ru
3/23/2011 8:59	0.cf7ts7.topmedicb.ru
3/23/2011 10:30	0.cf9.topmedicb.ru
3/23/2011 21:19	0.ct.medicsy.com
3/23/2011 22:42	0.cu60.medicsy.com
3/24/2011 2:52	0.d.medicsy.com

First Seen	Host/Domain
3/21/2011 10:43	candmedic.ru
3/19/2011 14:59	candoctor.ru
3/25/2011 12:14	candx.wke.asterwase.net
2/25/2011 10:58	cazht.medicinexi2.ru
3/29/2011 17:12	cazkt.extralegallow.org
1/28/2011 3:43	cazuy.pharmacyrx38.com

Places to get involved, help

- Mailing lists
 - Regops (see Rod)
 - NX-Domains (ask around)
 - Various trust groups
 - ICANN Compliance (RAA, Registry) or Security Team (Coordination, Technical) participate in many
- ICANN working groups
- FIRST (CERT teams)
- APWG, MAAWG, and other industry groups

You can't possibly remember all these hyperlinks!



So bookmark this page in your browser

<http://securityskeptic.com/the-security-skeptic/investigatingdnsabusejs.html> or

<http://safe.mn/FknC>

The background is a deep blue with abstract, lighter blue geometric shapes. A thin red arc is visible in the upper left. At the bottom, a portion of a globe is visible.

Thank You

Additional Questions