Passive DNS Evolution

presented by April Lorenzen

What is Passive DNS?

- DNS questions and answers are logged
- The collector doesn't decide what question is asked
- The collector passively collects the answers to DNS questions that are asked in the course of various general internet use
- Collected data is used for research purposes

Privacy?

- A passive DNS collector doesn't need to collect who asked the question

Example of data collected

Question: www.ISC.org

Answer: 204.152.184.88

- Is this publically available operational info?

Mining Passive DNS Data

- Discover some types of malicious activity
- Estimate technology adoption rates
- Observe the extent of DNS server configur-ation errors
- Academic research
- Law enforcement research

Successful Passive DNS Projects

- Florian Weimer's “Passive DNS Replication” project has been gathering data since 2004:
- http://www.enyo.de/fw/software/dnslogger/
- RUS-CERT has a limited public web interface for searching passive DNS data:
- http://cert.uni-stuttgart.de/stats/dns-replication.php

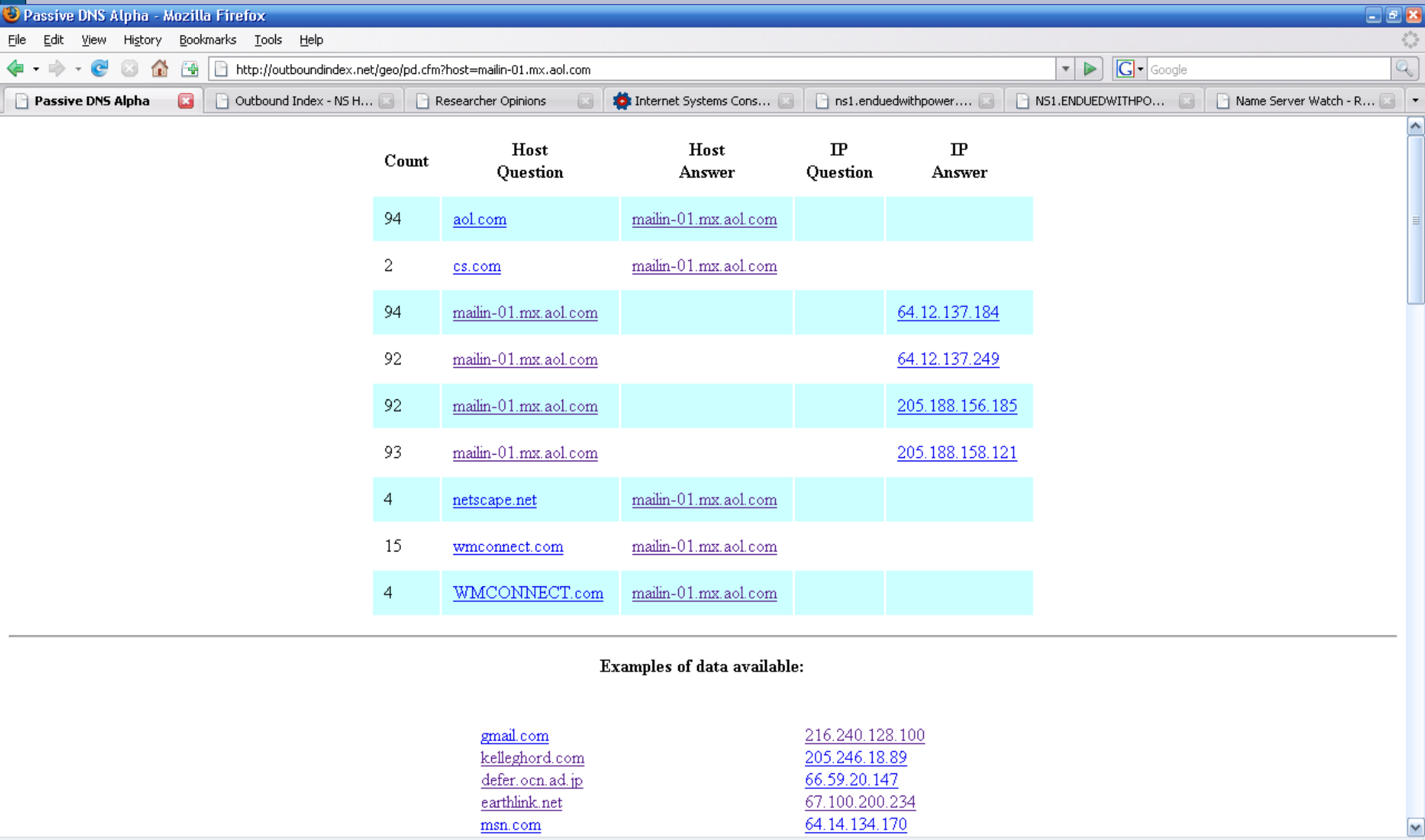
Current Uses of Florian's PDR

- Researchers look up resources used by a known malicious domain or IP
- Uncover related domains and IP addresses that are otherwise invisible
- Effective for discovering more about some phishing / malware / virus propagation
- Anti-spam research

ISC Passive DNS Collector Project Status

- Will provide non-public data to OARC members
- Expects to have a large number of collector contributor sites
- Test the alpha research interface here:
- http://outboundindex.net/geo/pd.cfm

Search Interface Screenshot



Count	Host Question	Host Answer	IP Question	IP Answer
94	aol.com	mailin-01.mx.aol.com		
2	cs.com	mailin-01.mx.aol.com		
94	mailin-01.mx.aol.com			64.12.137.184
92	mailin-01.mx.aol.com			64.12.137.249
92	mailin-01.mx.aol.com			205.188.156.185
93	mailin-01.mx.aol.com			205.188.158.121
4	netscape.net	mailin-01.mx.aol.com		
15	wmconnect.com	mailin-01.mx.aol.com		
4	WMCONNECT.com	mailin-01.mx.aol.com		

Examples of data available:

gmail.com	216.240.128.100
kelleghord.com	205.246.18.89
defer.ocn.ad.jp	66.59.20.147
earthlink.net	67.100.200.234
msn.com	64.14.134.170

Next Steps for ISC

- Scale up the ISC Passive DNS collector project
- More data, permanent web address for OARC members
- Continue improving searchability and speed as the data grows in size
- Listen to your feedback

Next Steps for You

- Use the alpha Passive DNS research tool and provide constructive feedback
- Contact ISC.org to become a collector site
- Software for collector contributors will be on the OARC server with the DSC software and various shell script helpers