DNS Firewalls with BIND: ISC RPZ and the IID Approach

Tuesday, 26 June 2012
About the Presenters

Paul Vixie
Chairman and Founder
Internet Systems Consortium

Rod Rasmussen
President and CTO
IID (Internet Identity)
Logistics

• Webinar is 1 hour long
• A recording will available in 3 business days at http://www.isc.org/webinars
• Participants are muted
• Use the Q&A Tab to submit questions
Agenda

• Building DNS Firewalls with RPZ – Paul Vixie
• DNS Firewall – Rod Rasmussen
• Q&A Session
Building DNS Firewalls
With RPZ

Paul Vixie
Internet Systems Consortium
DNS firewalls

- A DNS firewall examines responses to queries, passes some, blocks others.
- Responses can be “examined” for any content.
- “Block” action can discard, modify, or replace the original response.
The hard part

- The essence of a DNS firewall is simple.
- What’s hard? Maintenance.
- How to provide the data that guides its behavior?
- How to update that data easily?
- How to share that data with others?
More about RPZ

- DNS firewall rules carried inside DNS zones.
- Rules published, subscribed, shared by normal DNS zone transfer protocol
  - Including IXFR, NOTIFY, TSIG.
  - So, propagation is timely, efficient, and authentic.
RPZ inspection capabilities

• If the name being looked up is X.
• If the response contains any IP address in range X.
• If a listed name server name is X.
• If any returned name server IP address is in range X.
RPZ action capabilities

- Synthesize NXDOMAIN.
- Synthesize CNAME.
- Synthesize NODATA.
- Synthesize an answer.
- Answer with the truth.
Implications

- Controlled Balkanization.
- Open market for (many) producers and (many) consumers.
- Differentiated service at a global scale.
- Instantaneous takedown.
Status

- RPZ is open and unencumbered.
- Implemented only in BIND (so far).
- Performance reasonable (~15%).
- New features backward compatible.
- ISC standard not an IETF standard.
- We hope for other implementations.
DNS Firewalls

Rod Rasmussen
IID (Internet Identity)
President and CTO
Critical Internet Security Problems

- Malware command-and-control
- Malware infection sites
- APT attacks
- Phishing and spear phishing
Solution

- DNS Firewall
- Over 80% of malware uses DNS to communicate. Using a DNS firewall is an easy way to stop this.
- Network professionals and security pros working together for mutual benefit
- Leverages “big data” on Internet security events to create intelligence that prevents enterprise employee and system connections to known malicious Internet locations
- IID identifies and takes down thousands of malicious Internet locations a week
- Brings in data feeds and works with hundreds of global law enforcement, security vendors, security researchers
- Instantly alerts SOC/NOC of problems on enterprise networks via unique “TrapTrace” feature
Collective Intelligence

• Latest actionable intelligence on malicious Internet locations
• Share findings from unique customer relationships – one of the best networks around
• Aggregates many of the most robust threat intelligence streams in the industry
Feed Delivery

- Real-time threat updates via RPZ push capability
- Daily pre-determined malicious domains
- Feed empowers your own DNS infrastructure to provide robust security network wide with no new overhead
TrapTrace

- RPZ redirection enables enterprise security personnel to instantly be notified when a compromised machine tries to:
  - Access a command-and-control server
  - Transmit sensitive data to a known drop zone
  - Connect to spear phishing site
Use Cases: Malware and APT Attacks

- Malware command-and-control
- APT attacks
Summary

• Over 80% of malware uses DNS to communicate. Using a DNS firewall is an easy way to stop this.

• IID provides solution with actionable intelligence via RPZ feeds and unique TrapTrace feature

• By bridging gap between network administrators and security professionals, DNS firewalls are protecting real customers against real threats

• IID and ISC are ready to help
Take Action

- Go to www.internetidentity.com/solutions/activetrust-resolver
- Email dnsfirewall@internetidentity.com
Questions
About IID

Trust IID to proactively protect against the latest cyber threats:

• Five of the top six banks in the U.S.
• Largest government agencies worldwide
• Leading financial services firms, e-commerce, social networking and ISP companies

Headquartered in Tacoma, Washington

www.internetidentity.com
About ISC

- Non-profit dedicated to Internet infrastructure
- Software: BIND9, (BIND10,) ISC DHCP, ...
- Operations: F-Root, Hosted@ISC, ...
- Protocols: about two dozen IETF RFC’s
- Policy: Internet governance (e.g., SOPA)
- Commercial services:
  - support, training, feature development
  - registry services for new gTLD’s
  - DNS hosting (public-facing or “secondary”)