DNS Black Listing for Network Security

Melissa Muth
University of Pennsylvania

Matthew Wollenweber
The George Washington University
The Problem

Most Internet connections leverage Fully Qualified Domain Names (FQDNs) rather than IP addresses.

This makes browsing the web easier, but it also enable attackers to quickly change virtual hosts.
We Collectively Know the Malicious Sites

There are many resources that enumerate known bad domains such as:

- Malware Domain List
- Phish Tank
- Conficker Working Group
- Zeus Tracker
- SES
Leveraging the Collective Knowledge

- Aggregate all known malicious domains
- Proactively alter DNS records to point to a safe site
Normal DNS Traffic with an Attacker
DNS Filtering
Benefits

• Users can opt-in to the service
• Does not require network choke points
• Easy to deploy (via DHCP)
• Easy to opt-out
• Less invasive than a proxy service
• Cheaper and easier to use than a proxy
Questions

• What has been your impression/assessment of DNS sink holing until now?

• What would be your greatest concerns or challenges with implementing this on your campus?
Two Case Studies

- Penn: In-House system
- GWU: Managed solution - OpenDNS
University of Pennsylvania
The Case for a New Approach

• Polymorphic Malware
• 50% Effective AV Software
• 0-Day Threats
• Legitimate websites serving malicious 3rd party ads
The Case - Penn

Variably managed machines
Open perimeter
Implementation options

SANS + OpenDNS

In-house Proof of Concept

($)$
Implementation:
Domain Sources

SESv1
- SES: 95%
- MDL: 0%
- Zeus: 0%
- SRI: 4%

SESv2
- SES: 54%
- MDL: 45%
- Zeus: 2%
- SRI: 0%
Implementation - platform
Implementation - load

MySQL DB

BIND

MySQL DB

dns_records_1

dns_records_2

insert_2

Filtered domain list

MDL

SES

Zeus

Whitelist

Raw Domain List

Blacklist

named.conf

Thursday, May 17, 12
Implementation - communication

- Terms of Service
- Privacy Policy
- Documentation
- System build
- Maintenance
Performance - clients

- January 22, 2012
- February 5, 2012
- April 1, 2012
Performance: query/day
Performance

Malicious Portion of Requests

- Malicious
- Non-Malicious
Results

97% reduction in compromises

Monthly compromise %
Results - user experience

- No downtime
- Tertiary masked network outage
- False Positives
  - 3 from SRI (removed)
  - 2 from recently-cleaned domains
## Costs

<table>
<thead>
<tr>
<th>Out-of-pocket</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>$0</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td>$0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Build</td>
<td>2 person-weeks</td>
<td></td>
</tr>
<tr>
<td>Maintenance</td>
<td>30 min/mo</td>
<td></td>
</tr>
</tbody>
</table>
Lessons Learned

Not a replacement for campus DNS:

a value add
Lessons Learned - protocol

- DNSSEC
- TTL
Lessons Learned - privacy

Log as little as possible: domain request and referrer are sensitive
Lessons Learned

Branding matters:

vs

Thursday, May 17, 12
The Case

- Projects at GWU are incredibly slow - we needed a solution that could be implemented in a few months
- Network architecture has been organic and not centralized - proxies would be difficult
- Inline packet filtering - infeasible
The Case

- AV detection (at time of compromise) LESS THAN 30% (via Virus Total and SEP)
- Observed 70-80% correlation between the MDL and detected compromises
Vendor Selection and Deployment

- Few vendors appear to offer cloud based DNS filtering solutions
- Only OpenDNS met our requirements
  - Minimal TTL Increase (faster than GW)
  - High coverage of MDL
  - No obvious False Positives
  - Only malware blocked
- Deployment was via DHCP configuration
- Simple website to change OpenDNS settings
Configuration

Settings for: – Select an organization or network –

Dynamic IP addresses
OpenDNS supports networks ranging from single IP addresses, dynamic or static, on up to /16. Learn more about dynamic IPs.

Network verification
For individual IP addresses, verification is self-service, if you can click on a link from the network IP address. Networks larger than a single IP address are verified by OpenDNS employees reviewing account info and public records (like whois).

Shortcuts
Shortcuts are a cool way to use a short word for a long address.

Support Articles
- Generating Reports
- How do I Disable OpenDNS Completely?
- What is SmartCache?
Configuration

OpenDNS dashboard

Settings for: DIT Security

Web Content Filtering
- Security
- Customization
- Stats and Logs
- Advanced Settings

Users can contact you
Your users can contact you directly from the block page if they have questions. It'll show up as an email in your inbox.

Note about DNS forwarding
If you are forwarding requests to OpenDNS, domain blocking may not work properly if the domain's address is in your forwarder's cache.

Check a domain
Find out whether it would be blocked, and why.

Support Articles

Web Content Filtering

Choose your filtering level

- **Whitelist Only**
  - Enabling this feature will block all websites except those listed below under your "Never block" individual domains.

- **High**
  - Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters.

- **Moderate**
  - Protects against all adult-related sites and illegal activity.

- **Low**
  - Protects against pornography.

- **None**
  - Nothing blocked.

- **Custom**
  - Choose the categories you want to block.

Apply

Manage individual domains

Add/manage networks

26 categories in this group - View - Customize

13 categories in this group - View - Customize

4 categories in this group - View - Customize

Thursday, May 17, 12
Configuration

Web Content Filtering
Security
Customization
Stats and Logs
Advanced Settings

Security

Botnet Protection
- Enable botnet protection
  Enabling this option will stop known command and control hosts and websites from resolving on your network. We're continuously updating our database of known malicious hosts to keep you better protected online.

Malware Protection
- Enable malware protection
  Enabling this option will prevent known malware drop sites (sources of infection) from resolving on your network. We're constantly updating this list of websites in coordination with a number of other security organizations.

Internet-Scale Malware/Botnet Protection
- Enable basic malware/botnet protection
  Enabling this feature will protect your network from certain types of Internet-scale bots and wide-reaching malware, such as the Conficker virus and the Internet Explorer Zero Day Exploit. This is different from the Enterprise-class Malware and Botnet protection above. We recommend you enable it for added security.

Phishing Protection
- Enable phishing protection
  By enabling phishing protection, you’ll protect everyone on your network from known phishing sites using the best data available.
Configuration

Manage individual domains

If there are domains you want to make sure are always blocked (or always allowed) regardless of the categories blocked above, you can add them below.

- Always block

ADD DOMAIN

Add to all George Washington University networks

ALWAYS BLOCK:
1.bdl7qwj.ru
1.nwnudbg.ru
1.oooluq.ru
1800calculators.com
1x6a8lzwjx17jx8.com
2.cib3qwk.ru
2.vazqeef.ru
3.xy29fbf.ru
345.pl
60gp.ovh.net
8ahgiosgiso.nl.ai
9hz.com
Management

- Security maintains overall ownership of OpenDNS at GW
- Networking has full administrative rights
- Help desk can unblock any problem sites
- Administration can be delegated to appropriate parties - LSPs, Schools, etc
OpenDNS Performance

- Malware Coverage
  - MDL: 85% coverage*
  - SES: 88% coverage*
  - Others - similar
- Latency is less than local DNS servers
- False Positives
  - None reported via help desk in ~1 year
  - None detected via testing Alexia top 50k

*Exact “coverage” can vary on tolerance to protection versus potential problems. OpenDNS appears to fully ingest MDL, ShadowServer, CleanMX, Zeus Tracker, and other sources.
Unique IPs for George Washington University networks

April 1, 2012, to April 30, 2012

IPs
Total Requests for George Washington University networks
April 1, 2012, to April 30, 2012
Results
Results

- Deployment extended to most networks in Q1 2012
- 25% reduction between 2010 and 2011
- Currently running 80% reduced compromises from 2011
- On target to reduce detected compromises since 2010 by 87%
Results

• No complaints
• No downtime
• Little Effort
• More time to investigate less trivial traffic
Costs

- Hardware: [$0 - OpenDNS is cloud-based. No hardware needed.]
- Time: [Less than one week for deployment across all GWU locations. Cloud-based deployment is painless and quick.]
- Install, config, test software: [$0 - No software required.]
- Sporadic rebooting to apply patches [$0 - OpenDNS required no rebooting and no patching.]
- Time (ongoing): [$0 - OpenDNS requires no updates on GWU's end.]
- Annual service fee: Less than 100K
- Peace of mind and protection [Priceless]
- Avoiding GW internal development bureaucracy [Beyond priceless]
Other Factors

• OpenDNS is more reliable than internal DNS at GW - we peer with OpenDNS and have multiple uplinks but only two old DNS servers

• OpenDNS is a great vendor
  • We interact with their CEO
  • We interact with their technical folks
  • They fix our problems
  • If something isn’t perfect, they make it better
  • In short, this is perfect as a turn-key solution
Why Our Numbers aren’t Perfect

- Netwitness with Spectrum
- GFI Sandbox
- SourceFire IDS with Defense Center
- Dragon IDS
- DragonSlayer *in-house correlation and reporting*
- Centralized logging to Splunk including Firewall, AV, VPN logs
- Centralized Netflows
Conclusions

• We both continue to mutually prefer our specific solutions

• Audience thoughts?
Contact

- mwollenw@gwu.edu
- muthm@isc.upenn.edu