Malware Detection and Mitigation with Passive DNS and Blackhole DNS

Beth Young, MOREnet
youngba@more.net

David Wilhite, University of South Carolina
wilhite@sc.edu

April 4, 2011
DNS Analysis vs. Malware

How DNS Works
... and How Malware Uses DNS

presented by David Wilhite
How DNS Works

A? www.google.com

74.125.45.104

root/TLD nameservers
(fed by domain name registrations)

local nameserver

A? www.google.com

74.125.45.104

216.239.34.10

NS? google.com

google’s nameserver

216.239.34.10

www.google.com

74.125.45.104

user

A? www.google.com

74.125.45.104
Malware C&C

infected computer

123.30.40.50

A? cc.badguys.biz

local nameserver

123.30.40.1

NS? badguys.biz

root/TLD nameservers

malware C&C server

123.30.40.50

malware ISP nameserver

123.30.40.1
Malware C&C

avoiding local DNS blocks

infected computer

malware C&C server

malware ISP nameserver

local nameserver

root/TLD nameservers

NS? badguys.biz

A? cc.badguys.biz

123.30.40.1

123.30.40.50
Malware C&C

passing instructions via DNS

infected computer

malware ISP nameserver

root/TLD nameservers

NS? badguys.biz

123.30.40.1

TXT? cc.badguys.biz

A132EF8191A0B1C88EF5E
229900199A883A0B9D7F2
F1FF09A43D7

123.30.40.1
MOREnet’s BHDNS Service

Beth Young – youngba@more.net
Kris Trower – trower@more.net

EDUCAUSE Security Professionals
San Antonio
April 4, 2011
Agenda

• Introduction
• Implementation
• How the list is compiled and maintained
• Successes
Blackhole DNS

• Malware infection prevention
• Known malicious domains are blocked by intentionally poisoning DNS
• Service is free for our members

Cannot be used by non-member organizations or individuals.
The MOREnet BHDNS list

- Currently contains 325,000+ domains
- On average, we add 1,000+ new domains a day
- Our list is both proactive and reactive
- We have one FTE dedicated to the service
- Our removal request rate is .01%
  - Out of the 550,000 domains that have been listed, users requested the removal of 30.
New and Improved

• We have offered BHDNS for several years
• Originally had one source that wasn’t updated as frequently or as thoroughly as we had hoped
• We started compiling our own list in Feb. 2010
Why use it?

By preventing infections you save time and money.

- Fewer machines to clean
- Help prevent data loss/theft
- Prevent loss of productivity due to systems being infected
Is BHDNS a substitute for Antivirus software?

No!

- You should still run Antivirus software.
- We only blackhole domains we know about.
- Infections occur in many other ways.
- You will need a product to scan and clean infections when they do occur.
BHDNS Won’t Block...

- Malware accessed directly by IP
- Malware attachments sent in email
- Network aware worms
- Infected removable media
- High profile or critical sites that might be serving malware
- Major ad networks
  - May briefly block subdomains
How many members use it?

- About 360 MOREnet members
  - State government
  - Libraries
  - K12 schools
  - Technical schools
  - Colleges/Universities
  - Hospitals
- Through affiliation, many Universities across the U.S. also use the data
Blackholed Domains

• Previously resolved to internal loopback address 127.0.0.2
• Now resolve to web server blackhole.malwaredomains.more.net 207.160.130.67
• Enables us to gather statistics
• Resolves issues members with content filtering devices were having
What our users see

If the malicious domain leads to a web page:

“The requested page or advertisement has been blocked in accordance with local policies to prevent malware infection. If you feel this domain has been blocked in error, please contact your network administrator.”
The requested page or advertisement has been blocked in accordance with local policies to prevent malware infection. If you feel this domain has been blocked in error, please contact your network administrator.
What our users see

If the malicious domain leads to a graphic:

This image not available.
Additional Servers

- 4 caching servers that pull BHDNS data from a SQL server
  - BIND DLZ (Dynamically Loadable Zones)
  - Immediate additions and removals

- Prior to using a database we used text zone files with BIND
  - Zone file reload was taking up to an hour
  - During reload BHDNS resolution would default back to real IPs instead of loopback
Database

- Postgres
- Custom written procedure calls
- Look-ups optimized for quick return
Configuration

```sql
// {select domain from zones where domain = '$zone$'}

dlz "postgres zone" {
    database "postgres 2"
    {host=127.0.0.1 port=5432 dbname=blackhole user=bhdns}
    {select * from f_bhdns_zones('$zone$')}
    {select ttl, type, mx_priority, rvalue from f_bhdns_records('$zone$','$record$')}
    {} {}
    {}"
};
```
Mail servers

- We do not recommend using the BHDNS IP addresses for DNS resolution on your mail server
- Attempting to send email to blackholed domains could cause a mail loop (if using loopback address) or other issues
- If possible, configure mail servers to use standard DNS servers
Process

• Two Excel spreadsheets
  – One used for vetting
  – One used for cleaning up data with macros

• Domains are gathered from various feeds, blogs and websites and are cleaned up and added to the vetting spreadsheet.
Process

• Cleanup spreadsheet has several macros to clean up different types of data
• Macros remove everything but the domain... Including ‘www’ and IPs

keshande.com/updates/test.exe becomes keshande.com
Process

- Vetting spreadsheet uses conditional formatting
- Multiple tabs with different types of data
  - Current list of blacklisted domains
  - Whitelist
  - Alexa/Quantcast top 100,000
<table>
<thead>
<tr>
<th>#</th>
<th>Date</th>
<th>Domain</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>3067</td>
<td>3/24/2011</td>
<td>jqeytiwy.co.cc</td>
<td>Green</td>
</tr>
<tr>
<td>3068</td>
<td>3/24/2011</td>
<td>jxonquzj.co.cc</td>
<td>Green</td>
</tr>
<tr>
<td>3069</td>
<td>3/24/2011</td>
<td>kesfhtha.co.cc</td>
<td>Green</td>
</tr>
<tr>
<td>3070</td>
<td>3/24/2011</td>
<td>kpqqkorv.co.cc</td>
<td>Green</td>
</tr>
<tr>
<td>3071</td>
<td>3/24/2011</td>
<td>lbkdvxhu.co.cc</td>
<td>Green</td>
</tr>
<tr>
<td>3072</td>
<td>3/24/2011</td>
<td>lcpjhjhy.co.cc</td>
<td>Green</td>
</tr>
<tr>
<td>3073</td>
<td>3/24/2011</td>
<td>lfabbwkl.co.cc</td>
<td>Green</td>
</tr>
<tr>
<td>3074</td>
<td>3/24/2011</td>
<td>mbbckoua.co.cc</td>
<td>Green</td>
</tr>
<tr>
<td>3075</td>
<td>3/24/2011</td>
<td>google.com</td>
<td>Red</td>
</tr>
<tr>
<td>3076</td>
<td>3/24/2011</td>
<td>mgorytmk.co.cc</td>
<td>Green</td>
</tr>
<tr>
<td>3077</td>
<td>3/24/2011</td>
<td>mtkazbkd.co.cc</td>
<td>Green</td>
</tr>
<tr>
<td>3078</td>
<td>3/24/2011</td>
<td>mumqqhdb.co.cc</td>
<td>Green</td>
</tr>
<tr>
<td>3079</td>
<td>3/24/2011</td>
<td>myteenmovies.net</td>
<td>Green</td>
</tr>
<tr>
<td>3080</td>
<td>3/24/2011</td>
<td>nfasxerp.co.cc</td>
<td>Green</td>
</tr>
<tr>
<td>3081</td>
<td>3/24/2011</td>
<td>nvdshtnq.co.cc</td>
<td>Green</td>
</tr>
<tr>
<td>3082</td>
<td>3/24/2011</td>
<td>nvhxsnwb.co.cc</td>
<td>Green</td>
</tr>
</tbody>
</table>

Green – Already in database
Blue – Duplicate in today’s data
No color – New domain
Process

• Green domains: Left in list and uploaded so last seen date is updated.

• Blue domains: Left in list; ignored. Just a visual clue that domain has been listed by multiple sources.

• Red domains: Evaluated and removed if necessary.
Scripts

- At various times throughout the day, new domains are saved as a csv file and merged into the database using a script.
- We have several custom scripts to perform various functions:
  - Domain import
  - Domain remove
  - Whitelist import
  - Whitelist remove
Domain Import

• Performs checks before merging
  – Invalid characters? Error!
  – Missing period before TLD? Error!
  – Is domain on whitelist? Warning!
  – Is domain a TLD? Error!
  – All lowercase? If not, converted.
  – Domain already exists? If so, change last seen date.

• Merges all columns into the database.
Columns

• Date added
• Domain
• Source
• Proactive
• Date last seen
• A few other miscellaneous values
Whitelist Import

• Whitelist import
  – Individual domains from command line
  – Bulk list of domains from csv file
  – Includes source column
• Wildcarded Domains
  – *.google.com
  – No google.com subdomain will be blocked
Removal Scripts

• Domain remove
  – Individual domains from command line
  – Bulk list of domains from text file

• Whitelist remove
  – Individual domains from command line
  – Bulk list of domains from text file
Whitelist

- Contains Alexa top 10,000 global sites
- Quantcast top 10,000
- *.edu
- *.k12.mo.us
- *.gov
- Additional entries are gathered manually.
Whitelist

• There are malicious domains within the Alexa and Quantcast top 10,000

• These are removed from the whitelist when we find them
Removals

• Single domains are removed ASAP if we know the domain is a legitimate site that has been cleaned up.

• Domains that are expired or no longer resolve to an IP will be vetted for removal quarterly.

• Some feeds publish removal lists; Domains on these are removed weekly.
Removals - Annually

- Removals will be based on the Date Last Seen field.
- Domains that have not shown up after 1 year will be vetted for removal.
Proactive and Reactive

Proactive:
• Domains are found before they show up in the malware lists and research blogs.

Reactive:
• Domains are taken from aggregate lists, research blogs, AV vendors, private sources, member submissions, etc.
Proactive Data

- 1/2 to 3/4 of our daily additions are proactive finds.
- Domains added proactively are often added prior to their actual use.
- Some proactive domains are added weeks or months before their use, some just a matter of hours or days.
Reactive Data

- We monitor lists and feeds that publish known malicious domains.
- Lists with frequent false positives are checked as closely as possible.
- Monitoring malware lists helps us identify the patterns we use to proactively find bad domains.
Finding Proactive Domains

New domain registrations:

- Several sources of new domain registrations
  - dailychanges.com
  - domain-daily.com/downloads
  - tastereports.com

- Filter through thousands of new domains everyday

- Concentrate our efforts on registrars where we frequently see problematic domains
These match recent Zeus patterns:


1  abodylikebruce.com
2  abodylikebruce.net
3  evijmfmcvevfhcpp.info
4  gcepc.org
5  htmmwrrnnqpxwfl.biz
6  jzotvqqmyjvpmrr.org
7  lzotiltndusplj.org
8  webhonies.com
9  zriilzyolohrxch.info
Finding Proactive Domains

Bad registrars:

• Some registrars are rogue or cybercrime friendly
• We track some and single out for daily inspection
• We automatically shun Bizcn.com registrations
  – Kneber botnet; Mass Wordpress & GoDaddy attacks
  – TDSS/TDL3
  – Fake AV, malvertisemnets, etc.
• Found by tracking the registrars that register known malware
Finding Proactive Domains

Bad registrants:

• Individual registrant information is typically falsified

• Some are brazen enough to use the same information in all of their registrations:
  - Kneber botnet: Hilary Kneber
    hilarykneber@yahoo.com
  - TDSS/TDL3: Nmajjd Nbvjaa

• We know these registrations are malicious even if the domain doesn't fit any patterns
Finding Proactive Domains

Passive DNS:

• IPs and name servers that frequently host malware are tracked
• Passive DNS is used to find additional malicious hosts on the IP or name server
• Robtex is another good source
Are we sure all of the proactive domains are bad?

- Of those we find looking through new registrations, we are fairly certain.
- For the registrars we shun, there may be an occasional innocent causality.
- We look through the shunned domains to ensure there is nothing obviously critical.
- No one has ever requested that we remove one of the proactive domains.
The Kneber Botnet

- Named after its main registrant Hilary Kneber (HilaryKneber@yahoo.com)
- Mini Zeus crimeware botnet
- Involved in blackhat SEO
- New domains are added to our BHDNS list as they are registered

Kneber Examples

- dottasink.net added 06/11/2010
  Reported by Sucuri on 08/24/2010
- vancouvererrorsonfile.com added 05/16/2010
  Reported by Sucuri on 08/05/2010
- sparkspk.com added 08/30/2010
  Listed by Google Safe Browsing on 09/28/2010
- myblindstudionfoonline.com added on 09/13/2010
  Reported by Sucuri on 09/17/2010
- meqashopperinfo.com added on 09/23/2010
  Reported by Sucuri on 10/04/2010
TDSS/Alureon

- Rootkit that infects the master boot record
- Infests Windows system drivers
- Stealthy; Most anti-rootkit tools don’t detect it
- Botnets are sold on the black market
- Use depends on what ‘renters’ want to achieve
- New domains are added to our BHDNS list as they are registered
Mebroot

- Rootkit that replaces the master boot record
- Researcher asked for information on new Mebroot variant they noticed in late Feb. 2011
- We noticed the pattern in mid Nov. 2010
- We have been adding these domains as they are registered
SEO campaigns

- From May to mid September 2010, the .co.cc domain was popular for fake av registrations.
- Owned by a free subdomain redirection service out of Korea.
- Offer wildcard registrations that often appear as fakeproduct*.co.cc with * being replaced by a random number.
- Still a popular registrar, but use of this format seems to have declined.
- While they host thousands of evil domains, they also host legit ones.
Web Site Compromises

• Legitimate (sometimes popular) sites are compromised
  – Vulnerable Content Management software and plugins
  – Vulnerable applications and scripts
• Malicious URL is injected into source code
• Visitors are silently redirected to malware site
• Harden your website and keep it updated!
Fake AV Domains

• Still as prevalent as ever
• Block these if you are able!

*.co.cc   *.xe.cx
*.vv.cc   *.cx.cc
*.cz.cc   *.cw.cm
*.ce.ms   *.gv.vg
*.rr.nu   *.co.be
Zeus

- Tracking domain registrations that fit the Licat/Zeus pattern (since mid Oct. 2010)
- Pseudo-random domain names ending in .biz, .com, .net, .info and .org
  - kwqoutmkxpjvupsm.info
- Small percentage of them are showing up on Zeus Tracker or other malware lists
- Change registrars frequently
Malvertizing

• Major ad networks are doing a poor job of ensuring ads are malware free

• A large percentage of Fake AV malware is being pushed through ad networks

• Users going to perfectly acceptable sites are getting hit by drive-by downloads
Ad Blocking

Block them if you are able!

- By hostname and/or IP:
  http://pgl.yoyo.org/as/index.php

- Blocking Unwanted Parasites with a Hosts File:
  http://www.mvps.org/winhelp2002/hosts.htm

- Blocking with a browser plugin (Firefox):
  https://addons.mozilla.org/firefox/addon/1865

*Blocking ad servers is an excellent compliment to BHDNS.*
Deploying MVPS with Group Policy

Handout: Create GPO to install Hosts file on Windows 2008

DNS Analysis vs. Malware

Finding Malware Activity

presented by David Wilhite
Malware C&C

infected computer

A? cc.badguys.biz
123.30.40.50

local nameserver

A? cc.badguys.biz
123.30.40.1

NS? badguys.biz

root/TLD nameservers

malware C&C server

123.30.40.50

malware ISP nameserver

123.30.40.1
What We Can Watch For

infected computer

A? cc.badguys.biz

123.30.40.50

local nameserver

malware C&C server

123.30.40.50

malware ISP nameserver

123.30.40.1

root/TLD nameservers

Security sensors
How We Can Block This

infected computer

local nameserver

Blackhole DNS

malware C&C server

A? cc.badguys.biz

127.0.0.1

123.30.40.50
Malware’s Countermeasure

infected computer

A? cc.badguys.biz

local nameserver

Blackhole DNS

malware C&C server

123.30.40.50

127.0.0.1

But ... some malware species bypass local DNS ...
Malware C&C

avoiding local DNS blocks

infected computer

malware C&C server

123.30.40.50

malware ISP nameserver

123.30.40.1

root/TLD nameservers

123.30.40.1

NS? badguys.biz

123.30.40.1

A? cc.badguys.biz

123.30.40.50
What We Can Watch For

avoiding local DNS blocks

infected computer

malware C&C server

malware ISP nameserver

Security sensors

root/TLD nameservers

infected computer

NS? badguys.biz
123.30.40.1

A? cc.badguys.biz
123.30.40.50

malware C&C server
123.30.40.50

malware ISP nameserver
123.30.40.1
How We Can Block This

avoiding local DNS blocks

infected computer

malware C&C server

123.30.40.50

malware ISP nameserver

123.30.40.1

root/TLD nameservers

123.30.40.1

drop / null route

123.30.40.50

A? cc.badguys.biz

NS? badguys.biz

123.30.40.1
**Malware C&C**

passing instructions via DNS

infected computer

NS? badguys.biz

A132EF8191A0B1C88EF5E
229900199A883A0B9D7F2
F1FF009A43D7

TXT? cc.badguys.biz

123.30.40.1

malware ISP nameserver

123.30.40.1

root/TLD nameservers
How We Can Block All Of These

infected computer

malware C&C server

local nameserver

malware ISP nameserver

root/TLD nameservers

revoke domain registration

A? cc.badguys.biz
123.30.40.50

A? cc.badguys.biz
123.30.40.50

123.30.40.1

NS? badguys.biz
123.30.40.1

123.30.40.50

123.30.40.50
Malware’s Countermeasure

infected computer

local nameserver

malware C&C server

malware ISP nameserver

root/TLD nameservers

revoke domain registration

But ... some malware species use formulaic domain names ...
Malware's Countermeasure

How do you take down 500,000 possible domain names?

agsdjeys.com odjasurn.com ikqjfutm.com
poajehyt.com lhjqysmf.com kaheudhw.com
usjfhame.com magdfwus.com plqtdehg.com
qyudjane.com huejwdmc.com ajdncxsw.com
xsjhgwik.com jmkpogqs.com smcxdkop.com
wsjfhedk.com axkmeplk.com quijexjf.com
kkduhwjm.com oequnaxl.com xjudlkme.com
oklejfn.com dxakmrhg.com ... etc ...
Detection and Analysis

**Torpig/Mebroot**
- 8-formula-alpha (dot) com
- querying root servers
  - afaijklw.com
  - uahskdja.com
  - nwghjkas.com
  - kaollwsa.com

**Bredolab**
- encoded-values-in-hostname

(details under NDA)

**Atypical Behavior**
- large numbers of bad queries
- queries to known evil nameservers
- results that indicate evil nameserver
- queries to root servers
- (and more)
Identifying Local Threats

**Malware Analysis**
- antivirus-one-care2010.com
- ebuntosakert.com
- live-pc-care.com
- live-pccare.com
- one-care-antivirus.com
- pc-live-care2010.com
- pc-livecare2010.com
- pc-live-care.com
- pc-livecare.com
- security-pccare.com
- securitypc-care.com
- securitypccare.com
- windows-live-care.com

**Phishing Reports**
- www.web-ppl-cmd.com
- 9hz.com
- klemin.org

**Exposure to Risk**
(19,000+ listed malicious sites)
- 2600warez.net
- liveprotection.net
- youtube19.com
- facebook-pics.info
Signature-Based Detection

Bredolab - Timestamped DNS Queries - seen on router: core

query of form: (encoded-values) . (some-domain)
made to servers: any
query result: any
min hits displayed: 1
confidence level: High
counterindications: none known

Queries Client IP (PTR)  -------  ------------------------------------
2 10.254.32.3 (UNKNOWN) 10.254.32.0/30, Student Wireless VPN Pool  
[encoded].gevaeus.com [encoded].grosta.com  
4 172.20.135.26 (UNKNOWN) 172.20.135.0/27, [location redacted]  

Torpig/Mebroot - 8.3 Root Queries - seen on router: core

query of form: 8-alpha dot 3-alpha
made to servers: root
query result: any
min hits displayed: 1
confidence level: Medium - evaluate before acting
counterindications: non-random domain names are false positives

Queries Client IP (PTR)  -------  ------------------------------------
2 129.252.79.19 ([redacted].sc.edu) 129.252.79.0/24, College of [redacted]  
fillserv.com tanyetta.com
<table>
<thead>
<tr>
<th>Client IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>129.252.139.237 (UNKNOWN)</td>
</tr>
<tr>
<td>129.252.157.140 (UNKNOWN)</td>
</tr>
<tr>
<td>129.252.229.31 (UNKNOWN)</td>
</tr>
<tr>
<td>129.252.82.101 (UNKNOWN)</td>
</tr>
<tr>
<td>172.17.125.115 (UNKNOWN)</td>
</tr>
<tr>
<td>172.20.66.118 (UNKNOWN)</td>
</tr>
</tbody>
</table>
### Standard Server Statistics - seen on router: core

**client count per server**

<table>
<thead>
<tr>
<th>Clients</th>
<th>Server IP (PTR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3502</td>
<td>172.27.7.112 (cae145dnsp02.ds.sc.edu)</td>
</tr>
<tr>
<td>2591</td>
<td>172.27.7.115 (cae145dnsp01.ds.sc.edu)</td>
</tr>
<tr>
<td>1433</td>
<td>172.27.7.116 (cae145gsp01.ds.sc.edu)</td>
</tr>
<tr>
<td>1195</td>
<td>172.27.7.113 (cae145adcp02.ds.sc.edu)</td>
</tr>
<tr>
<td>1180</td>
<td>129.252.42.25 (name1.sc.edu)</td>
</tr>
<tr>
<td>1059</td>
<td>129.252.41.11 (name0.sc.edu)</td>
</tr>
<tr>
<td>279</td>
<td>129.252.1.168 (psyc.cla.sc.edu)</td>
</tr>
<tr>
<td>94</td>
<td>129.252.251.14 (ns-ext2.sc.edu)</td>
</tr>
<tr>
<td>85</td>
<td>172.27.7.122 (cae145adcp07.ds.sc.edu)</td>
</tr>
<tr>
<td>40</td>
<td>172.27.7.123 (cae145adcp08.ds.sc.edu)</td>
</tr>
<tr>
<td>34</td>
<td>129.252.74.104 (SchPubHealth-NS1)</td>
</tr>
<tr>
<td>32</td>
<td>208.67.222.222 (resolver1.opendns.com)</td>
</tr>
<tr>
<td>30</td>
<td>172.27.5.212 (cosslaruffalo.csd.sc.edu)</td>
</tr>
<tr>
<td>29</td>
<td>129.252.251.12 (ns-ext1.sc.edu)</td>
</tr>
<tr>
<td>21</td>
<td>8.8.8.8 (google-public-dns-a.google.com)</td>
</tr>
<tr>
<td>20</td>
<td>172.27.7.124 (cae145adcp09.ds.sc.edu)</td>
</tr>
<tr>
<td>17</td>
<td>129.252.74.105 (SchPubHealth-NS2)</td>
</tr>
<tr>
<td>15</td>
<td>64.134.255.2 (custcache00.wayport.net)</td>
</tr>
<tr>
<td>13</td>
<td>208.67.220.220 (resolver2.opendns.com)</td>
</tr>
<tr>
<td>12</td>
<td>129.252.158.10 (ns-mail1.sc.edu)</td>
</tr>
<tr>
<td>11</td>
<td>65.55.37.62 (ns1.msft.net)</td>
</tr>
<tr>
<td>11</td>
<td>4.2.2.2 (vnsc-bak.sys.gtei.net[UNKNOWN])</td>
</tr>
<tr>
<td>10</td>
<td>64.4.59.173 (ns2.msft.net)</td>
</tr>
</tbody>
</table>
Nonstandard Server Statistics - seen on router: core

<table>
<thead>
<tr>
<th>Client count</th>
<th>Server IP (PTR)</th>
<th>Clients:</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>202.12.28.131 (ns3.apnic.net)</td>
<td>129.252.143.140</td>
<td>129.252.143.148</td>
<td>129.252.143.95</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>200.3.13.11 (ns2.lacnic.net)</td>
<td>129.252.143.140</td>
<td>129.252.143.148</td>
<td>129.252.143.95</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>192.31.80.30 (d.gtld-servers.net)</td>
<td>10.130.2.175</td>
<td>129.252.184.149</td>
<td>129.252.81.12</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>198.41.0.4 (a.root-servers.net)</td>
<td>10.89.13.40</td>
<td>129.252.81.12</td>
<td>129.252.81.38</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>192.42.93.30 (g.gtld-servers.net)</td>
<td>129.252.19.10</td>
<td>129.252.81.12</td>
<td>172.17.40.10</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>192.228.79.201 (b.root-servers.net)</td>
<td>129.252.104.42</td>
<td>129.252.81.38</td>
<td>129.252.97.208</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>64.211.42.193 (UNKNOWN)</td>
<td>10.130.2.175</td>
<td>129.252.19.10</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>93.188.162.65 (93.188.162.65.static.ukrtelegroup.com.ua[UNKNOWN])</td>
<td>[10.135.20.3]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>93.188.162.226 (93.188.162.226.static.ukrtelegroup.com.ua[UNKNOWN])</td>
<td>[10.135.20.145]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>93.188.161.205 (93.188.161.205.static.ukrtelegroup.com.ua[UNKNOWN])</td>
<td>[10.135.20.3]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>156.154.71.22 (UNKNOWN)</td>
<td>[129.252.79.91]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>156.154.70.22 (UNKNOWN)</td>
<td>[129.252.79.91]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Behavioral Analysis

### Client DNS Promiscuity Statistics

Top 100 clients server count on nonstandard servers - seen on router: core

<table>
<thead>
<tr>
<th>Servers</th>
<th>Client</th>
<th>------- --------------------------</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>129.252.81.12 (UNKNOWN)</td>
<td>servers: 128.63.2.53 156.154.105.25 156.154.128.70</td>
</tr>
<tr>
<td>19</td>
<td>10.130.2.175 (UNKNOWN)</td>
<td>192.203.230.10 200.31.69.107 216.239.34.10 216.239.36.10 216.239.38.10 66.196.84.168 98.136.43.32</td>
</tr>
<tr>
<td>12</td>
<td>129.252.19.10 (NOISY-pacs.med.sc.edu)</td>
<td>servers: 192.112.36.4 192.31.80.30 198.6.1.142 198.6.1.146</td>
</tr>
<tr>
<td>12</td>
<td>129.252.81.38 (UNKNOWN)</td>
<td>servers: 192.112.36.4 192.31.80.30 198.6.1.142 198.6.1.146</td>
</tr>
<tr>
<td>10</td>
<td>172.17.123.10 (pegasus.esri.sc.edu)</td>
<td>servers: 63.95.218.156</td>
</tr>
<tr>
<td>7</td>
<td>129.252.184.149 (NOISY-RussellHouse)</td>
<td>servers: 192.228.79.201 192.31.80.30 192.33.4.12 192.5.6.36</td>
</tr>
<tr>
<td>6</td>
<td>129.252.97.208 (NOISY-ope.ed.sc.edu)</td>
<td>servers: 129.252.116.54 (UNKNOWN)</td>
</tr>
<tr>
<td>5</td>
<td>129.252.116.54 (UNKNOWN)</td>
<td>servers: 204.13.250.26 204.13.251.26 208.78.70.26 208.78.71.26</td>
</tr>
<tr>
<td>4</td>
<td>10.89.13.40 (UNKNOWN)</td>
<td>servers: 198.41.0.4 199.249.112.1 64.27.65.13</td>
</tr>
<tr>
<td>3</td>
<td>10.135.20.167 (UNKNOWN)</td>
<td>servers: 192.203.230.10 192.42.93.30</td>
</tr>
<tr>
<td>3</td>
<td>10.135.20.12 (UNKNOWN)</td>
<td>servers: 192.228.79.201 192.31.80.30 192.33.4.12 192.5.6.36</td>
</tr>
<tr>
<td>2</td>
<td>129.252.79.91 (ga91.geol.sc.edu)</td>
<td>servers: 156.154.70.22 156.154.71.22</td>
</tr>
<tr>
<td>2</td>
<td>129.252.24.57 (aleroldan-pc.ce.sc.edu)</td>
<td>servers: 143.248.1.177 143.248.2.177</td>
</tr>
<tr>
<td>2</td>
<td>129.252.176.157 (UNKNOWN)</td>
<td>servers: 205.152.132.23 205.152.37.23</td>
</tr>
<tr>
<td>2</td>
<td>129.252.143.95 (UNKNOWN)</td>
<td>servers: 200.3.13.11 202.12.28.131</td>
</tr>
<tr>
<td>2</td>
<td>129.252.143.148 (UNKNOWN)</td>
<td>servers: 200.3.13.11 202.12.28.131</td>
</tr>
<tr>
<td>2</td>
<td>129.252.143.140 (UNKNOWN)</td>
<td>servers: 200.3.13.11 202.12.28.131</td>
</tr>
<tr>
<td>2</td>
<td>10.254.64.19 (UNKNOWN)</td>
<td>servers: 207.69.188.186 207.69.188.187</td>
</tr>
</tbody>
</table>
Behavioral Analysis

Query Statistics

top 100 hostnames queried - seen on router: core
clients per queried hostname

<table>
<thead>
<tr>
<th>Clients</th>
<th>Hostname</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>3822</td>
<td>wpad.sc.edu (UNKNOWN)</td>
<td>(143.215.203.39)</td>
</tr>
<tr>
<td>3512</td>
<td>osceX-en.url.trendmicro.com</td>
<td>(143.215.203.39)</td>
</tr>
<tr>
<td>3329</td>
<td><a href="http://www.google-analytics.com">www.google-analytics.com</a></td>
<td>(74.125.65.139)</td>
</tr>
<tr>
<td>3304</td>
<td><a href="http://www.google.com">www.google.com</a></td>
<td>(74.125.47.106)</td>
</tr>
<tr>
<td>3206</td>
<td>ad.doubleclick.net</td>
<td>(74.125.47.149)</td>
</tr>
<tr>
<td>3013</td>
<td>wpad.ds.sc.edu (UNKNOWN)</td>
<td>(74.125.47.149)</td>
</tr>
<tr>
<td>2859</td>
<td>s0.2mdn.net</td>
<td>(74.125.47.149)</td>
</tr>
<tr>
<td>2789</td>
<td><a href="http://www.facebook.com">www.facebook.com</a></td>
<td>(69.63.189.16)</td>
</tr>
<tr>
<td>2735</td>
<td>view.atdmt.com</td>
<td>(65.242.27.34)</td>
</tr>
<tr>
<td>2673</td>
<td><a href="http://www.update.microsoft.com">www.update.microsoft.com</a></td>
<td>(65.55.185.26)</td>
</tr>
<tr>
<td>2631</td>
<td>b.scorecardresearch.com</td>
<td>(143.215.203.14)</td>
</tr>
<tr>
<td>2602</td>
<td>download.windowsupdate.com</td>
<td>(65.54.95.140)</td>
</tr>
<tr>
<td>2589</td>
<td>static.ak.fbcdn.net</td>
<td>(143.215.203.16)</td>
</tr>
<tr>
<td>2566</td>
<td>googleads.g.doubleclick.net</td>
<td>(74.125.47.156)</td>
</tr>
<tr>
<td>2480</td>
<td>clients1.google.com</td>
<td>(74.125.47.102)</td>
</tr>
<tr>
<td>2452</td>
<td>ad.yieldmanager.com</td>
<td>(98.136.154.148)</td>
</tr>
<tr>
<td>2412</td>
<td>pixel.quantserve.com</td>
<td>(64.94.107.25)</td>
</tr>
<tr>
<td>2315</td>
<td>spe.atdmt.com</td>
<td>(143.215.203.33)</td>
</tr>
<tr>
<td>2293</td>
<td><a href="http://www.sc.edu">www.sc.edu</a></td>
<td>(129.252.189.62)</td>
</tr>
<tr>
<td>2123</td>
<td>pagead2.googlesyndication.com</td>
<td>(74.125.47.165)</td>
</tr>
<tr>
<td>2103</td>
<td>profile.ak.fbcdn.net</td>
<td>(143.215.203.33)</td>
</tr>
<tr>
<td>2039</td>
<td><a href="http://www.googleadservices.com">www.googleadservices.com</a></td>
<td>(74.125.47.96)</td>
</tr>
</tbody>
</table>
Behavioral Analysis

Bad Query Statistics

top 100 hostnames not found - seen on router: core
clients per queried hostname

<table>
<thead>
<tr>
<th>Clients</th>
<th>Bad Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>333</td>
<td>wpad (UNKNOWN)</td>
</tr>
<tr>
<td>182</td>
<td>internalcheck.apple.com (UNKNOWN)</td>
</tr>
<tr>
<td>73</td>
<td>i.qai.cdn.turner.com (UNKNOWN)</td>
</tr>
<tr>
<td>57</td>
<td>isatap.sc.rr.com (UNKNOWN)</td>
</tr>
<tr>
<td>49</td>
<td>s1.4publishers.com (UNKNOWN)</td>
</tr>
<tr>
<td>47</td>
<td><a href="http://www.1-affordable-california-health-insurance.com">www.1-affordable-california-health-insurance.com</a> (UNKNOWN)</td>
</tr>
<tr>
<td>40</td>
<td>google.lucidmedia.com (UNKNOWN)</td>
</tr>
<tr>
<td>36</td>
<td>images.fullaudio.com (UNKNOWN)</td>
</tr>
<tr>
<td>27</td>
<td>TMSLA1.uscd.rc (UNKNOWN)</td>
</tr>
<tr>
<td>24</td>
<td>usinfo.state.gov (UNKNOWN)</td>
</tr>
<tr>
<td>23</td>
<td>srv203.ole.itec (UNKNOWN)</td>
</tr>
<tr>
<td>23</td>
<td>ipv6.labs.wikimedia.org (UNKNOWN)</td>
</tr>
<tr>
<td>22</td>
<td>wpad.uscd.rc (UNKNOWN)</td>
</tr>
<tr>
<td>19</td>
<td><a href="http://www.csiseason.com">www.csiseason.com</a> (UNKNOWN)</td>
</tr>
<tr>
<td>18</td>
<td><a href="http://www.jameswolcott.com">www.jameswolcott.com</a> (UNKNOWN)</td>
</tr>
<tr>
<td>18</td>
<td>cn1.redwoosh.akadns.net:443 (UNKNOWN)</td>
</tr>
<tr>
<td>17</td>
<td>favicon.ico (UNKNOWN)</td>
</tr>
<tr>
<td>17</td>
<td>bi-lostage.corp.bi-lo.com (UNKNOWN)</td>
</tr>
<tr>
<td>16</td>
<td>familydollar.co (UNKNOWN)</td>
</tr>
<tr>
<td>15</td>
<td>crossdomain.xml (UNKNOWN)</td>
</tr>
<tr>
<td>15</td>
<td>TMFS3.csd.ec.edu (UNKNOWN)</td>
</tr>
</tbody>
</table>
## Misguided Client Statistics

**top 100 clients making bad queries - seen on router: core**

<table>
<thead>
<tr>
<th>Bad Queries</th>
<th>Client IP (PTR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3366</td>
<td>99.3% 172.20.185.10 (UNKNOWN)</td>
</tr>
<tr>
<td>2466</td>
<td>95.2% 172.20.240.146 (UNKNOWN)</td>
</tr>
<tr>
<td>1380</td>
<td>52.5% 129.252.106.168 (UNKNOWN)</td>
</tr>
<tr>
<td>1095</td>
<td>85.8% 129.252.221.167 (UNKNOWN)</td>
</tr>
<tr>
<td>1075</td>
<td>31.1% 10.144.226.2 (UNKNOWN)</td>
</tr>
<tr>
<td>1066</td>
<td>59.2% 10.31.19.85 (UNKNOWN)</td>
</tr>
<tr>
<td>859</td>
<td>52.1% 172.20.64.174 (UNKNOWN)</td>
</tr>
<tr>
<td>632</td>
<td>71.7% 172.17.27.93 (UNKNOWN)</td>
</tr>
<tr>
<td>455</td>
<td>6.6% 129.252.189.65 (NOISY-carbon.csd.sc.edu)</td>
</tr>
<tr>
<td>424</td>
<td>85.1% 129.252.210.9 (NOISY-cuda.music.sc.edu)</td>
</tr>
<tr>
<td>326</td>
<td>29.4% 10.254.64.13 (UNKNOWN)</td>
</tr>
<tr>
<td>292</td>
<td>48.7% 10.254.64.2 (UNKNOWN)</td>
</tr>
<tr>
<td>230</td>
<td>58.1% 10.254.64.21 (UNKNOWN)</td>
</tr>
<tr>
<td>186</td>
<td>26.3% 10.250.100.150 (itso-bunyan.csd.sc.edu)</td>
</tr>
<tr>
<td>119</td>
<td>92.2% 129.252.164.77 (UNKNOWN)</td>
</tr>
<tr>
<td>97</td>
<td>6.5% 129.252.92.186 (UNKNOWN)</td>
</tr>
<tr>
<td>67</td>
<td>0.4% 10.236.6.2 (UNKNOWN)</td>
</tr>
<tr>
<td>61</td>
<td>48.0% 10.30.55.224 (UNKNOWN)</td>
</tr>
<tr>
<td>46</td>
<td>1.8% 10.30.50.252 (UNKNOWN)</td>
</tr>
<tr>
<td>45</td>
<td>2.3% 129.252.250.208 (UNKNOWN)</td>
</tr>
<tr>
<td>44</td>
<td>1.9% 10.30.53.171 (UNKNOWN)</td>
</tr>
<tr>
<td>43</td>
<td>4.0% 10.31.20.216 (UNKNOWN)</td>
</tr>
<tr>
<td>18</td>
<td>1.2% 129.252.112.239 (UNKNOWN)</td>
</tr>
</tbody>
</table>
Searching for evil DNS servers

combining DNS log files for 2010-07-14

finding benchmark IP addresses (narrowed to CIDR /24 networks)

benchmarks:
\t.trendmicro\com,|,teredo\ipv6\microsoft\com,|urs\microsoft\com,|
\tdownload\microsoft\com,|\windowsupdate\com,|\symanetc\com,|\symanetcliveupdate\com,|geo\yahoo\com,|companion\yahoo\com,|\ceipmsn\com,|ak\imgfarm\com,

169 right answers

finding same lookups by nonstandard nameservers

removing right answers

done

144.135.8.182 @AU (UNKNOWN)
oscex-en.url.trendmicro.com

208.44.108.136 @US (208-44-108-136.dia.static.qwest.net)
backup.nfc.trendmicro.com
backup21.url.trendmicro.com
csm50.nfc.trendmicro.com
osce10-p.activeupdate.trendmicro.com
oscex-en.url.trendmicro.com
OS Fingerprinting

if($3 ~ /^wpad$/) { print $1",win","$3 } 
if($3 ~ /^wpad\$/) { print $1",win","$3 } 
if($3 ~ /download\.windowsupdate\.com$/) { print $1",win","$3 } 
if($3 ~ /update\.microsoft\.com$/) { print $1",win","$3 } 
if($3 ~ /^time\.windows\.com$/) { print $1",win","$3 } 
if($3 ~ /^dell-alive/) { print $1",win","$3 } 
if($3 ~ /^internalcheck\.apple\.com$/) { print $1",mac","$3 } 
if($3 ~ /time\.apple\.com$/) { print $1",mac","$3 } 
if($3 ~ /^iphone-maps\.apple\.com$/) { print $1",iapp","$3 } 
if($3 ~ /^iphone-services\.apple\.com$/) { print $1",iapp","$3 } 
if($3 ~ /^iphone-wu\.apple\.com$/) { print $1",iapp","$3 } 
if($3 ~ /\.playstation\.net$/) { print $1",ps3","$3 } 
if($3 ~ /\.update\.playstation\.org$/) { print $1",ps3","$3 } 
if($3 ~ /metrics\.us\.playstation\.com$/) { print $1",ps3","$3 } 
if($3 ~ /^avatar\.xboxlive\.com$/) { print $1",xbox","$3 } 
if($3 ~ /download\.xbox\.com$/) { print $1",xbox","$3 } 
if($3 ~ /download-ssl\.xbox\.com$/) { print $1",xbox","$3 } 
if($3 ~ /XETGS\.XBOXLIVE\.COM$/) { print $1",xbox","$3 }
if($3 ~ /^ntp\..ubuntu\..com$/) { print $1",linux,"$3 }
if($3 ~ /^archive\..ubuntu\..com$/) { print $1",linux,"$3 }
if($3 ~ /^changelogs\..ubuntu\..com$/) { print $1",linux,"$3 }
if($3 ~ /^security\..ubuntu\..com$/) { print $1",linux,"$3 }
if($3 ~ /centos\..pool\..ntp\..org$/) { print $1",linux,"$3 }
if($3 ~ /fedora\..pool\..ntp\..org$/) { print $1",linux,"$3 }
if($3 ~ /opensuse\..pool\..ntp\..org$/) { print $1",linux,"$3 }
if($3 ~ /^xmlrpc\..rhn\..redhat\..com$/) { print $1",linux,"$3 }
DNS Analysis vs. Malware

Implementing Your Program

presented by David Wilhite
Implementing Detection

1. Gain the backing of organization policy.
   a) Do you have the authority to observe and collect DNS data?
   b) What privacy protections must you implement?
2. Establish infrastructure for tapping DNS traffic.
   a) Use IDS sensors? taps? spans? DNS server logs?
   b) Establish server to collect and correlate data.
3. Leverage existing intelligence sources.
4. Analyze DNS traffic.
5. Lurk and learn.
   a) False positives?
   b) Exposure vs. post-infection behavior.
   c) Is this an infected client, or a DNS server for an infected client?
1. Gain the backing of organization policy.
   a) Do you have the authority to notify and/or block?
   b) What privacy protections must you implement?
   c) What NDA data must you protect?

2. Establish procedure for mitigation.
   a) Who are the contacts to notify?
   b) Create notification templates.
   c) When do you block? Who can be blocked, and who cannot?
   d) Who will do the cleaning?
   e) When do you unblock?
   f) Create a feedback mechanism to evaluate effectiveness.

3. Implement your mitigation strategy.
   a) Start with a segment not critical to business operations.
   b) Watch for false positives, and revise detection criteria.
   c) Expand scope as practical.
Malware Detection and Mitigation with Passive DNS and Blackhole DNS

Beth Young, MOREnet
youngba@more.net
David Wilhite, University of South Carolina
wilhite@sc.edu

April 4, 2011