Argonne NATIONAL LABORATORY

ProActive DNS Blacklisting

Gene Rackow
Argonne National Laboratory

The Basics of DNS

Hostname to IP mapping and back

Host aliases

Mail server locations

Services

Security records

What is DNS Blacklisting?

DNS Blacklist also known as a DNS Blackhole.

Local server fakes zones know to contain:

- Malware
- Spyware
- Command/Control
- Advertising
- Political Issues

What are DNS Blacklist Benefits

Preventing hosts from getting to bad stuff.

If you are not presented with the malware,

Chances are you are not going to be infected.

Estimates are that blocking Advertising sites stops 85% of infections.

DNS Blacklist Sources of information

- MalwareDomains
- Abuse.CH
  - SpyEyeTracker
  - ZeusTracker
- Dshield
- CyberFedModel
- JC3
  - Tippers
  - Radar
- Master Blocking List

Bad News about DNS Blacklisting

Typically It's ReActive.

Entries are added AFTER something happened.

Some machines have already been

- Infected
- Inspected
- Dissected
- Reported

How to become PROactive

Zeus Tracker posting several new sites daily

What is common about these sites

- Hostnames look like randomsplatter.com
- Typically registered days before use
- Registered by one of several people
  - Nmajjd Nbvjaa, Yamir Jayantila, Dik Loren

Common Registrar of BIZCN.COM Inc

Track changes at the Registrar

Tracking sources

- TasteReports
- DailyChanges

Between 3 and 50 new domains a day.

- now 100’s to 1000’s/day

Checking New Entry Usage

- Few if any hits from lab machines
  - Commonly incidental hits off
    - news sites (mostly foreign)
    - blogs
    - wikis
- Within a week several sites added to
  - Zeustracker
  - MalwareDomains

More Registrars

CNMSN.com (97,000 domains)

DNS-DIY.net (300,000 domains)

CSCdns.net (176,000 domains)

Tracking DNS Servers

FreeWebDNS.com (32 domains)

HoperJoper.ru (11 domains)

Internet.bs (73 domains)

Registerdomain.name (78 domains)

You're now asking: Does it work?

Jan 24, Weekly "632" JC3 Site Call

Details on digging into "new" malware.

Hosting and/or C&C indicated 28 hosts

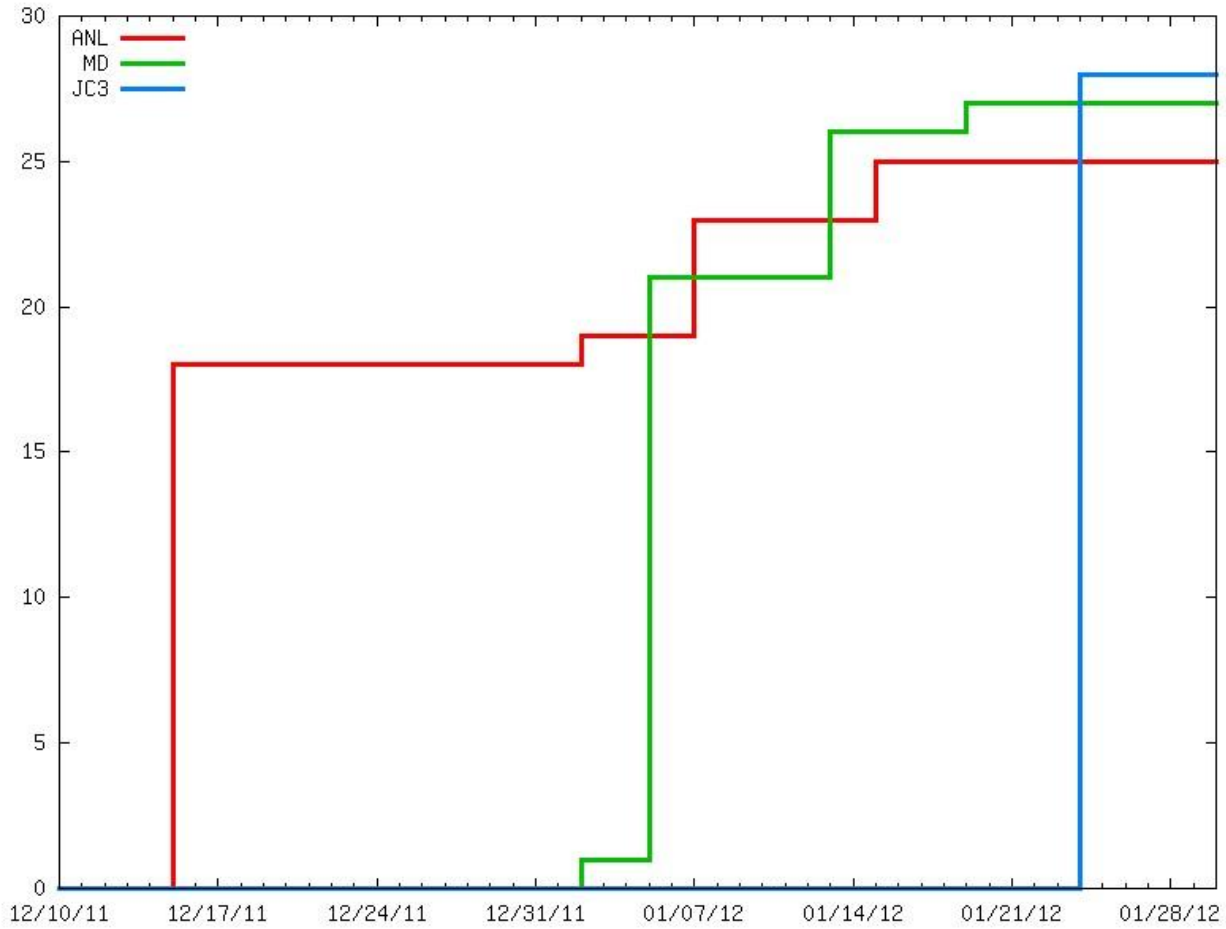
27 were already blacklisted at ANL

25 from Registrar diving

2 additional from other sources

Only 1 "new" host

Blocking Timeline



Tipper 1 on April 2.

Details

Malicious IP:
65[.]75[.]146[.]185

Domain Names:
Sweepstakeslovers[.]com
Nickelbackre[.]com
Yelowardoneye[.]com
Sendprefic[.]com

Malicious Code:
Generic FakeAlert.bz, a variant of Win32/Kryptik.ANDY,
Supicious.cloud.5, or Heuristic.LooksLike.Win32.Winwebsed.B

Last 3 domains Blocked on Mar 22

Tipper 2 on April 2

Details

Malicious IP:

188[.]62[.]171[.]7
64[.]120[.]207[.]106
64[.]120[.]207[.]99
66[.]33[.]197[.]137

Domain Names of Attacker:

Familymoneymaking[.]net
Golddefence[.]net
Homeworkingnow[.]net
Moneymakingeasy[.]net

2 Domains Blocked on March 28

Sharing the Data

Details being pushed to

- Cyber Fed Model
- Master Blocking List

Questions?

Comments?

Nap Time?