Tracking A Zombie Army

James Lick

jlick@jameslick.com
What Is It?

- Millions of compromised hosts
  - Viruses, Trojans, Spyware, Backdoors,
    Worms, etc.

- Spammers use them to send spam
- CBL detects and blocks infected hosts
- Only indirect evidence this happens

‘Atriks’ claims they are used with permission
How to track it?

• It’s impossible!!!
• No, it’s just very, very difficult.
• The evidence is there if you have
  – Luck
  – A Search Warrant or Subpoena
  – Plenty of resources
• Lots of other crimes are very difficult to solve
My DNS server is attacked

• My in.named process was eating CPU
• My bandwidth was higher than normal
• Lots of queries from 206.81.95.113 and 206.81.95.115
• All queries are MX queries
• Oops! I had an “Open DNS Server”
  – Recursion was open to all
Securing the server

- Turn off recursion to outside hosts:

  acl internal {
    192.168.168.0/24;
    66.92.182.240/28;
  };

  options {
    allow-recursion { internal; };
  };

- Firewall out the attackers:
  - block in from 206.81.80.0/20 to any
What just happened?

- Why all these lookups?
  - Attacking me?
  - Spammering people?
  - Distributing viruses?
- Who was attacking?
  - 206.81.80.0/20 is AceTech USA
    - Spamhaus says they are mortgage spammers
  - 206.81.95.0/24 is Clear Tech Services
- How can I find out more?
How to find out more

• Could I give bogus results and see what happens?
• How can I give bogus results to these clients?
• Could BIND 9’s view feature help me lie?
• How do I make this all work?
• What will happen?
Configuring BIND to lie

- BIND 9 has ‘view’ feature
- ‘view’ is usually used for ‘Split DNS’
  - Hide internal hosts from the Internet without running multiple servers
- Make an ACL of who you want to lie to:

  acl attackers {
    206.81.80.0/20;
  };

Designing the fake view

• Make a ‘fake’ view first in the file:

```plaintext
view "fake" {
    match-clients { attackers; };
    recursion no;
    zone "." {
        type master;
        file "static/fake.named.root";
    };
    zone "com" {
        type master;
        file "static/fake.named.com";
    };
};
```
Fake zone examples

• Add in a fake ‘root’ or ‘.’ zone:

  . IN SOA dns.shoreside.com. jlick-dns.drivel.com. ( 
    1 1800 900 259200 3600 )
  IN NS dns.shoreside.com
dns.shoreside.com IN A 66.92.182.248

• Add in a fake “com” zone:

$ORIGIN .
$TTL 86400
com IN SOA dns.shoreside.com. jlick-dns.drivel.com. ( 
  11 1800 900 259200 3600 )
  IN NS dns.shoreside.com
dns.shoreside.com IN A 66.92.182.248
.*.com IN MX 10 smx1.tcp.com
Make a view for regular zones

• Add your regular zones in a view last, so it will be the fall-through default:

```plaintext
view "real" {
    match-clients { any; };

    zone "." {
        type hint;
        file "static/named.root";
    };

    ...
};
```
See what happens next…

• Within seconds, hundreds of systems from all over the world start calling
• Most of them already known zombies on the CBL list
• sendmail on that system melts down
• Everything is bounced, so I don’t know the content of the mail
Collecting mail attack data

• Looking at available ‘honeypot’ software for collecting mail sessions, most is inefficient and fragile
• Chris Lewis of Nortel has a patched version of postfix’s smtp-sink which offers more logging
• Smtp-sink is a very efficient multi-threaded C program, and stood up to the challenge
Spamhaus was right!

• Typical spam sample collected:
  – HELO <my-ip-address>
  – “If you are paying more than 3.6% on your mortgage, we can slash your monthly payment!”
  – URL in gogetdealz.com domain
  – Not CAN-SPAM compliant
    • Forged headers, no opt-out, no mailing address, etc.
Some more questions arise

• Who was doing the A queries?
  – Only one or two A queries seen for my MX
  – A queries coming from another “Open DNS” server
  – Zombie controllers are doing all lookups and passing info on to the zombies

• Who is Clear Tech Services?
  – Servers in Spokane, WA, USA
  – Company in Columbia, TN, USA
  – Tried contacting by phone, but not interested in talking to me
More questions (cont)

• Who is gogetdealz.com?
  – On address 219.148.62.226
  – Located in Shijiazhuang, Hebei, PRC
  – On China Telecom network
  – Multiple Spamhaus SBL listings
    • Male anatomy pills, Mortgage ‘bank’, “#1 source for reliable bullet-proof services”
  – All domains linked to ns[123].33122.biz DNS servers
Zombie Army Architecture
Conclusions

- Careful monitoring of suspicious DNS patterns can reveal abuse
- Disinformation can reveal inner workings
- It is possible to find who is working in the shadows
- Law enforcement can do even more research
- More analysis of data collected is needed