Passive DNS

Using the DNS for fun and profit

Alexandre Dulaunoy

January 25, 2013

Domain Name Space and Structure 1/3

- The domain name space is structured in a tree.
- The DNS root zone is at the top and provide information on how to reach top-level domains (ccTLD, gTLD).
- Security is limited and DNSSEC is not currently largely deployed.

Name Servers Roles 2/3

- Authoritative name server
  - Give answers about domain name configured by the local name administrator.
- Recursive and caching name server
  - They recursively lookup domains by querying and caching to/from authoritative name server.
- It's recommended to keep separated the authoritative name server from the recursive name server.

DNS Protocol 3/3

```
▾ Queries
  ▾ scribe.twitter.com: type A, class IN
      Name: scribe.twitter.com
      Type: A (Host address)
      Class: IN (0x0001)
▾ Answers
  ▸ scribe.twitter.com: type CNAME, class IN, cname api.twitter.com
  ▸ api.twitter.com: type A, class IN, addr 128.242.250.157
  ▸ api.twitter.com: type A, class IN, addr 199.59.148.30
  ▸ api.twitter.com: type A, class IN, addr 199.59.148.32
  ▸ api.twitter.com: type A, class IN, addr 128.242.245.189
▸ Authoritative nameservers
```

- DNS uses UDP or TCP over port 53. The core element for the DNS procotol is the RR (Resource Record). Each record is composed of various fields: NAME, TYPE, CLASS, TTL, RDLENGTH and RDATA.

DNS and Security?

- Everyone relies on DNS on Internet even malware.
- Can we monitor DNS passively to discover malware infection or limiting its impact?
  - First passive DNS implemented in 2004 by Florian Weimer.
  - Discovering of malware fast-flux domains, malicious domains/IP, hijacked domains...
  - Privacy is critical when doing passive DNS.

DNS and Security - Quick Workshop

- From simple DNS monitoring to dnscap (https://github.com/adulau/dnscap).
- Can you use the DNS queries/answers for network forensic analysis?
- How to abuse DNS? DNS (cache, query) poisoning.
- DGA? fast-flux? how are those techniques used by malware?

dnscap - how to use it

- dnscap -g -i eth0 $\rightarrow$ dump decode queries/answers for DNS
- dnscap -g -i eth0 -s r $\rightarrow$ dump DNS answers only

Bibliography

- DNS and BIND, Fifth Edition, Cricket Liu, Paul Albitz.
- Passive Monitoring of DNS Anomalies, Bojan Zdrnja, Nevil Brownlee, and Duane Wessels.

Q and A

- Thanks for listening.
- adulau@foo.be