nominet®

Monitoring DNS?
Analysing DNS!

Roy Arends
Research Fellow
Nominet UK

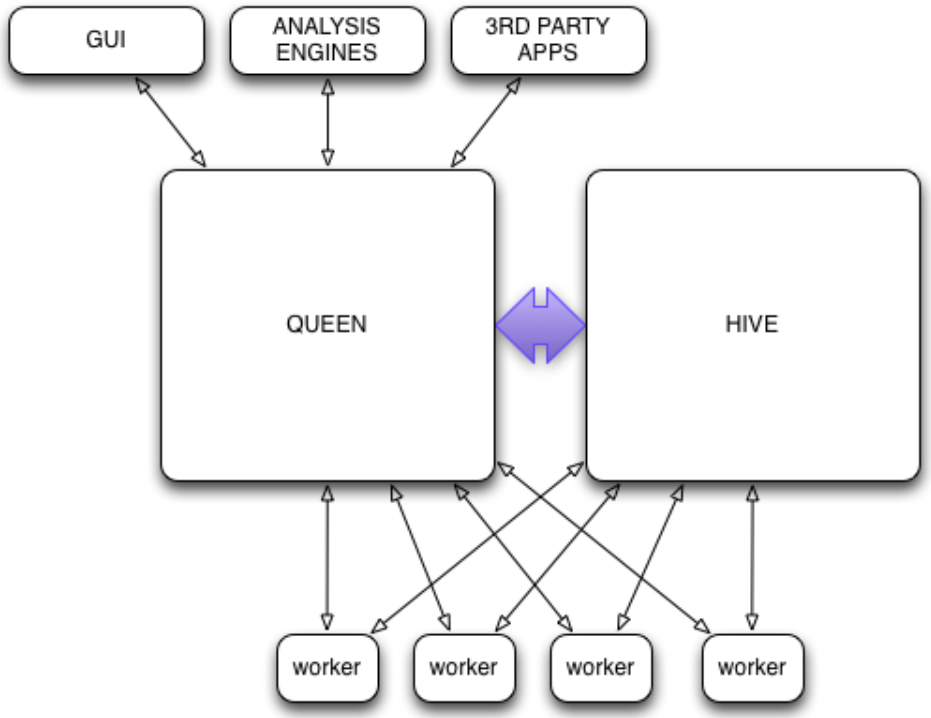
nominet®

What is Monitoring?

- Monitoring hints at an incident
  (what is happening)
- Analysing is the actual hard work
  (why is it happening)

Technology

- BumbleBee has been built from the ground up with a bespoke patent-pending architecture that outperforms all other Big Data alternatives, such as Hadoop, Cassandra and other NoSQL databases for large volumes of DNS data.

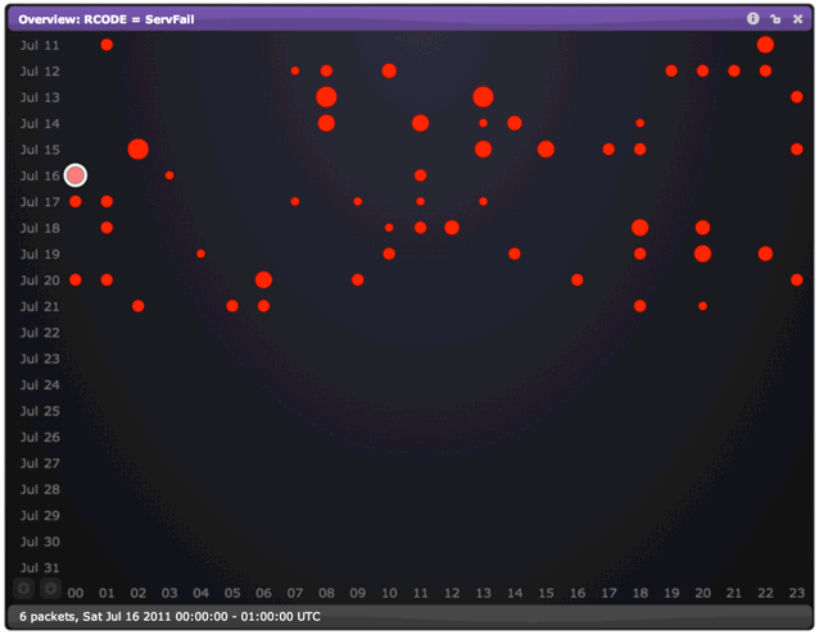


nominet®

ANALYSIS CASE STUDIES

The Google Bug

- BB noticed a lot of SERVFAIL responses
- BB revealed that this was due to
  - Very long domain names (larger than 255 bytes)
  - Which was not protocol compliant
  - All came from a specific set of addresses
- This was GOOGLEs 8.8.8.8 DNS Service
  - Making resolving difficult for their end users
- We informed them July 11th, 2011, they fixed it on July 21st, 2011



- SERVFAIL is actually the wrong error code
- Hence, this was also a bug in BIND
- We informed ISC in 2013
- This was fixed in the next release of BIND

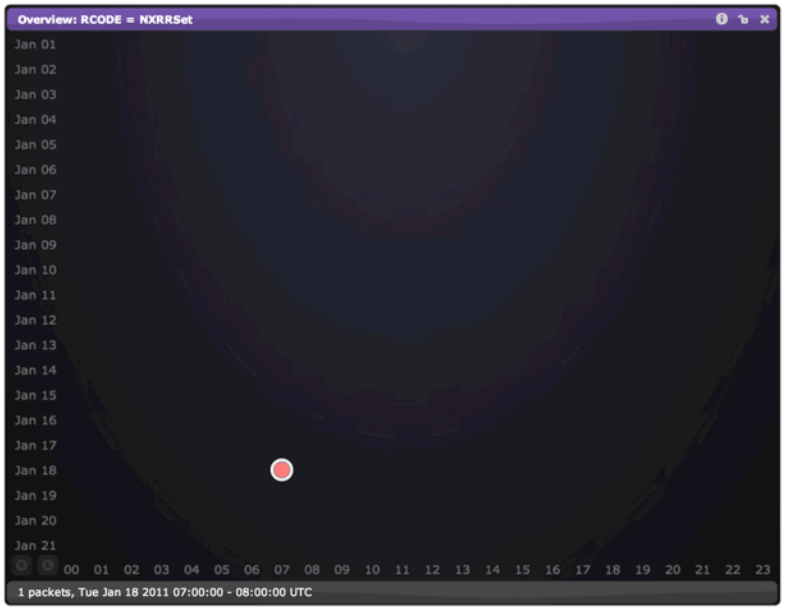
OpenDNS problems

- BB showed a lot of re-query traffic from OpenDNS (Bursts)
  - they just kept asking, as if they never got a response
  - Over and Over and Over
  - From all their Singapore based servers
- We notified them July the 8th 2011
- Fixed on July the 9th 2011

- OpenDNS waited only 300 ms for a response
- The latency was 160 ms on average
- Round trip time is thus 320 ms
- Too late for OpenDNS, they just re-sent the query

Packet of Death

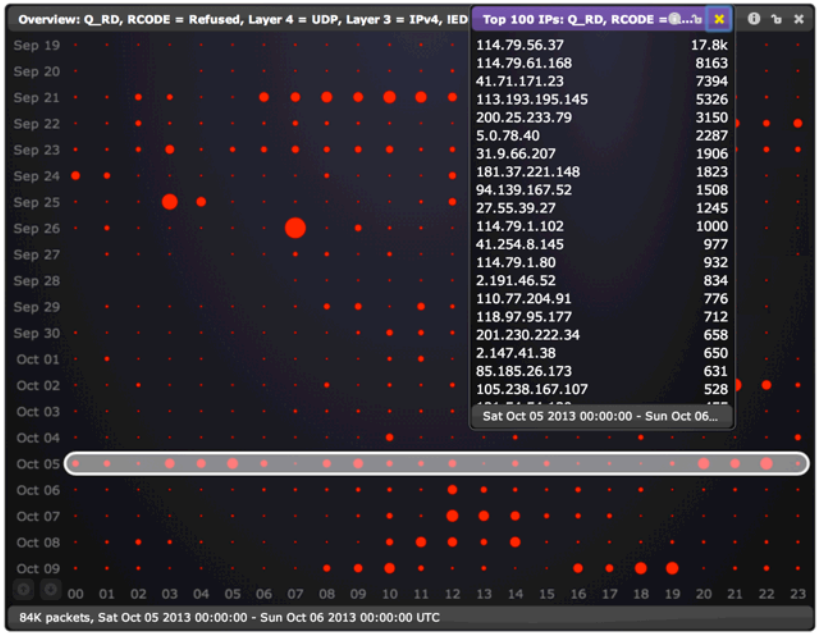
- BIND is capable of a lot of functions
  - Dynamic update, Continuous Signing, Resolving
- Our Nameservers have no need for them
  - They act as Authoritative (no resolving)
  - They act as Secondaries (no dynamic updates)
- Hence, we should never see related behavior in Bumblebee
  - must always see REFUSED for update attempts
- Our servers never showed related behavior.
- With one exception:
- A dynamic update on Jan 18th, 2011 7:03 am
- Lead to an NXRRSET response
  - This should be a REFUSED response
- BB found a single needle in a very large haystack



- This specific dynamic update was benign
- The source address was sending random data to our servers
- However, we should never allow this through
  - Should be REFUSED instead of NXRRSET
- A slightly modified packet stops all modern versions of BIND
- This lead to CVE-2011-2464 & 2465

The Cutwail Botnet

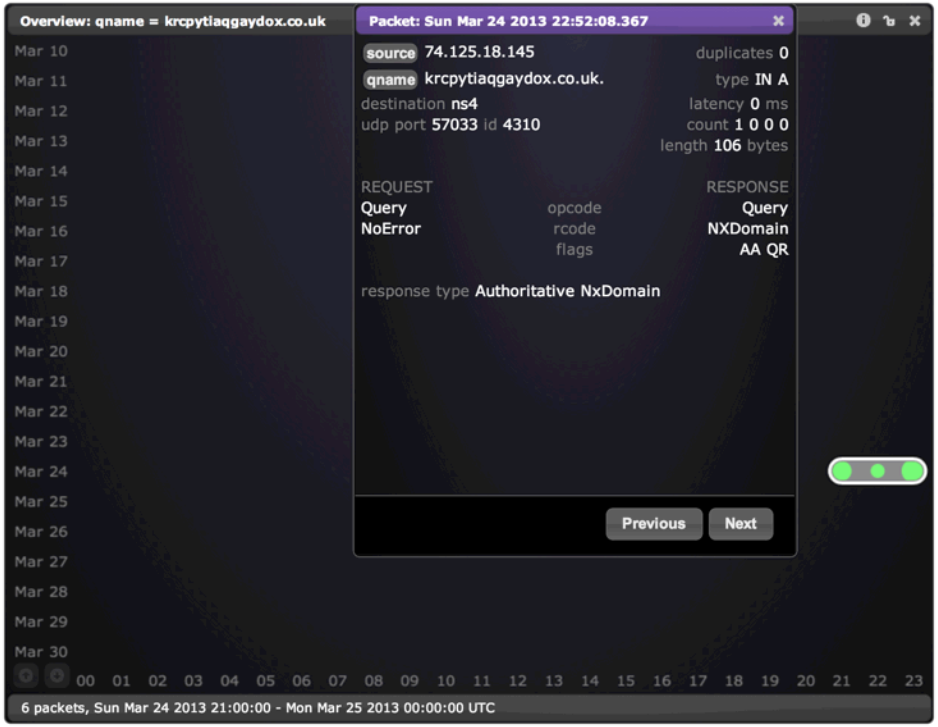
- BB showed a large amount of MX requests
- Deeper investigation showed that
  - Most were for non-existent mail addresses
  - Most had the RD bit set
  - All of the above did not query for anything else
  - Only queried for a short, irregular period of time
  - All had low query identifiers
  - Some asked for names we don't know about
- Using Bumblebee, a very specific fingerprint was developed.
- This fingerprint identifies new infections very quickly
- This has lead to spam-block-lists
- Has the potential to reduce the amount of spam in the UK



The Index Case

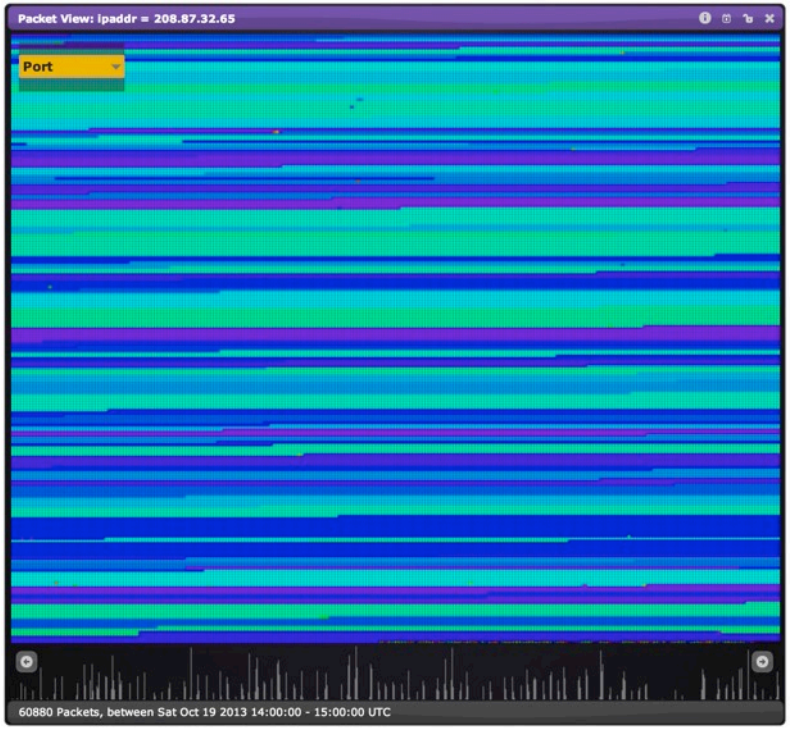
- Cryptolocker is very aggressive malware
- It contacts the botmaster using a DGA
  - Domain Generating Algorithm
  - Unique set of UK domains per day
  - Known Algorithm, so trivial to predict
  - Botmaster registers a single domain in the future
- Over time, more and more infections
- This works out the other way as well by Going back in time
- In epidemiology, the index case is the initial patient showing symptoms of an infection
  - Aka "Patient Zero"
- We generated all possible domains for every single day since january 1st 2012.
- The very first hit was on march 24th 2013

  krcpytiaqgaydox.co.uk
- Additional data confirms that cryptolocker creators are experimenting, starting that day



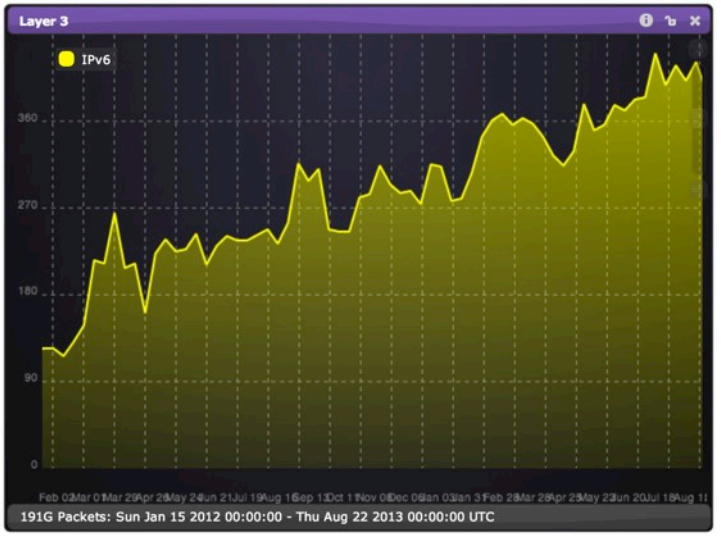
Not That Random

- In DNS, source ports should be randomly chosen
  - To avoid Kaminsky style blind spoofing/ cache poisoning attacks
  - Also the identifier should be randomly chosen
- Bumblebee can trivially show that this is not the case for any arbitrary address at any time
- The example shows that the resolver does not choose its ports at random



Take-up of IPv6 & DNSSEC

- In 18 months time
  - use of IPv6 has quadrupled
  - use of DNSSEC has trippled.
- Bumblebee shows
  - IPv6: 100 qps in Jan ’12
  - IPv6: 400 qps in Aug ‘13
  - DNSSEC: 40 qps Jan ’12
  - DNSSEC: 120 qps Aug ‘13



nominet®

Why analysis is important

- Without analysis, you're left in the dark during an incident
- What appears to be an attack (lots of traffic) is often a misconfiguration
  - (never attribute to malice that which is adequately explained by stupidity)
- Monitoring the health of the system is often left to nagios (or the like)
  - Threshold alarms
    - Raise alarm when X is over 80%
  - CPU/MEM/NETWORK/DISK usage
    - Nice graphs that no-one looks at, until a threshold alarm is raised
- Analysing the traffic is far more powerful and informative than monitoring arbitrary system data.