Monitoring DNS? Analysing DNS!

Roy Arends Research Fellow Nominet UK



- 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.





## **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 11<sup>th</sup>, 2011, they fixed it on July 21<sup>st</sup>, 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 8<sup>th</sup> 2011
- Fixed on July the 9<sup>th</sup> 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 18<sup>th</sup>, 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

Overview	/: Q	_RD,	RCO	DE =	Refu	sed,	Layer	4 =	UDP,	Laye	er 3 =	IPv4	, IED	То	p 100	IPs:	Q_R	D, RC	ODE	=0	љ 1	•	<b>0</b> 1	, x
Sep 19														114	.79.5	56.37					17.8	k		
Sep 20														114	.79.6	51.16	8				816	3		
Sep 20														41.	71.17	1.23					739	4		
Sep 21														113	.193	.195.	145				532	6		•
Sep 22														200	.25.2	233.7	9				315	ю		•
														5.0	78.4	0					228	7		
Sep 23														31.9	9.66.	207					190	6		•
Sep 24														181	.37.2	221.1	48				182	3		•
Sec. 25														94.:	139.1	67.5	2				150	8		
Sep 25				-										27.	55.39	9.27					124	5		
Sep 26														114	.79.1	.102					100	0		•
Sep 27														41.3	254.8	3.145					97	7		
oop ar														114	.79.1	.80					93	2		1
Sep 28														2.19	91.46	5.52					83	4		18
Sep 29														110	.77.2	204.9	1				77	6		
Sec. 20														118	.97.9	95.17	7				71	2		
Sep 30														201	.230	.222.	34				65	8		89
Oct 01														2.14	17.41	1.38	-				65	0		2 • I
Oct 02														85.	185.4	0.1/	3				63	1		•
000002														105	.238	16/.	10/				52	8		
Oct 03														Sat Oct 05 2013 00:00:00 - Sun Oct 06										
Oct 04		•									•													•
Oct 05	•	٠	٠			۲	٠	•	٠	٠	٠	٠	•	•	٠	٠	٠	٠	٠	٠		٠		
Oct 06													•											
Oct 07															•									
Oct 08												-												•
Oct 09																								•
000																								23
84K pack	ets,	Sat	Oct 0	5 201	3 00:0	00:00	- Sun	Oct	06 20	13 00	0:00:0	о ито												

#### 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 1<sup>st</sup> 2012.
- The very first hit was on march 24<sup>th</sup> 2013 krcpytiaqgaydox.co.uk
- Additional data confirms that cryptolocker creators are experimenting, starting that day

Overview: qname = krcpytiaqgaydox.co.uk	Packet: Sun Mar 24 2013 22:52:08.367	/ ×	<b>0</b> ъх						
Mar 10	source 74.125.18.145	duplicates 0							
Mar 11	qname krcpytiaqgaydox.co.uk.	type IN A							
Mar 12	destination ns4	latency 0 ms							
Mar 13	udp port 57033 id 4310	count 1000							
Mar 14		lenger 100 bytes							
Mar 15	REQUEST	RESPONSE							
	Query opcode	Query							
Mar 16	flags	AA OR							
Mar 17									
Mar 18	response type Authoritative NxDoma	in							
Mar 19									
Mar 20									
Mar 21									
Mar 22									
Mar 23									
Mar 24									
Mar 25									
Mar 26	Pre	vious Next							
Mar 27									
Mar 28									
Mar 29									
Mar 30									
0 00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	16 17 18 19	20 21 22 23						
6 packets, Sun Mar 24 2013 21:00:00 - Mon Mar 25 2013 00:00:00 UTC									

#### 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







#### 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.