janet

BOTNETS ON LARGE NETWORKS

James Davis, UKNOF26

@JanetCSIRT

BACKGROUND

IP EXPLOSION

janet

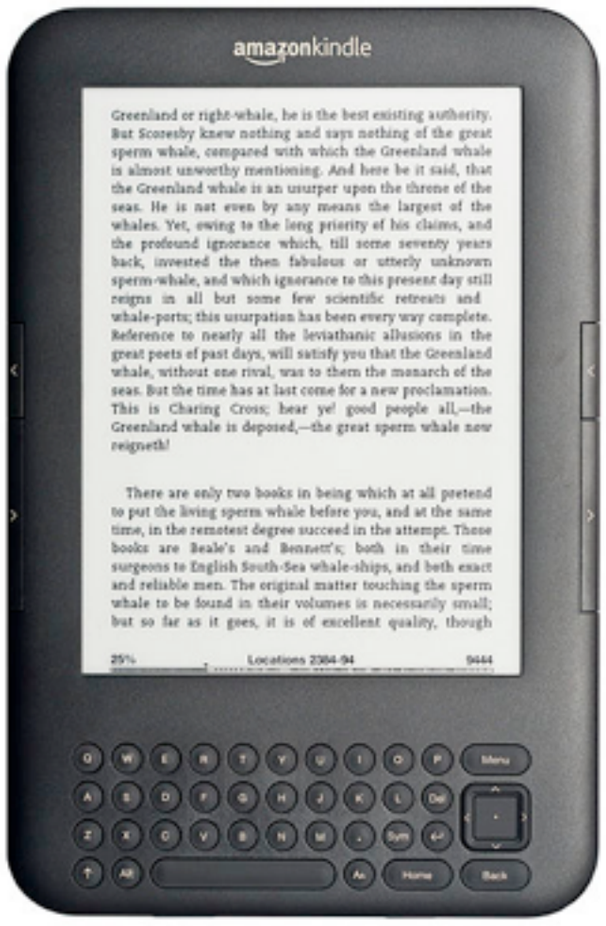
IP is getting everywhere... students BYOEverything. Yesterday:

@JanetCSIRT

IP EXPLOSION

janet

Today:



@JanetCSIRT

IP EXPLOSION

janet

Tomorrow:

@JanetCSIRT

IP DEVICES

janet

- Most companies making IP enabled x, are manufacturers of x, not networking companies
- Security, especially network security won't be a factor in their design or support

@JanetCSIRT

IP AS RIGHT

janet

- Students expect Internet access, everywhere.
- Universities are ranked on "student experience"
- Overly draconian IT policies will be counterproductive

- What happens if you block the institution's VLE?
- What happens if you block an IP fridge from the network?
- What happens if you block an IP pacemaker from the network?

- Can Janet make that call?

@JanetCSIRT

THE BIG PICTURE

janet

- Growing numbers of devices that vendors owners don't consider "computers"
- Security of these devices will not be supported by vendors or owners.
- Most of these devices are unmanageable
- Many of these systems are vulnerable
- So some portion of them of them will end in botnets

@JanetCSIRT

STATE OF PLAY

janet

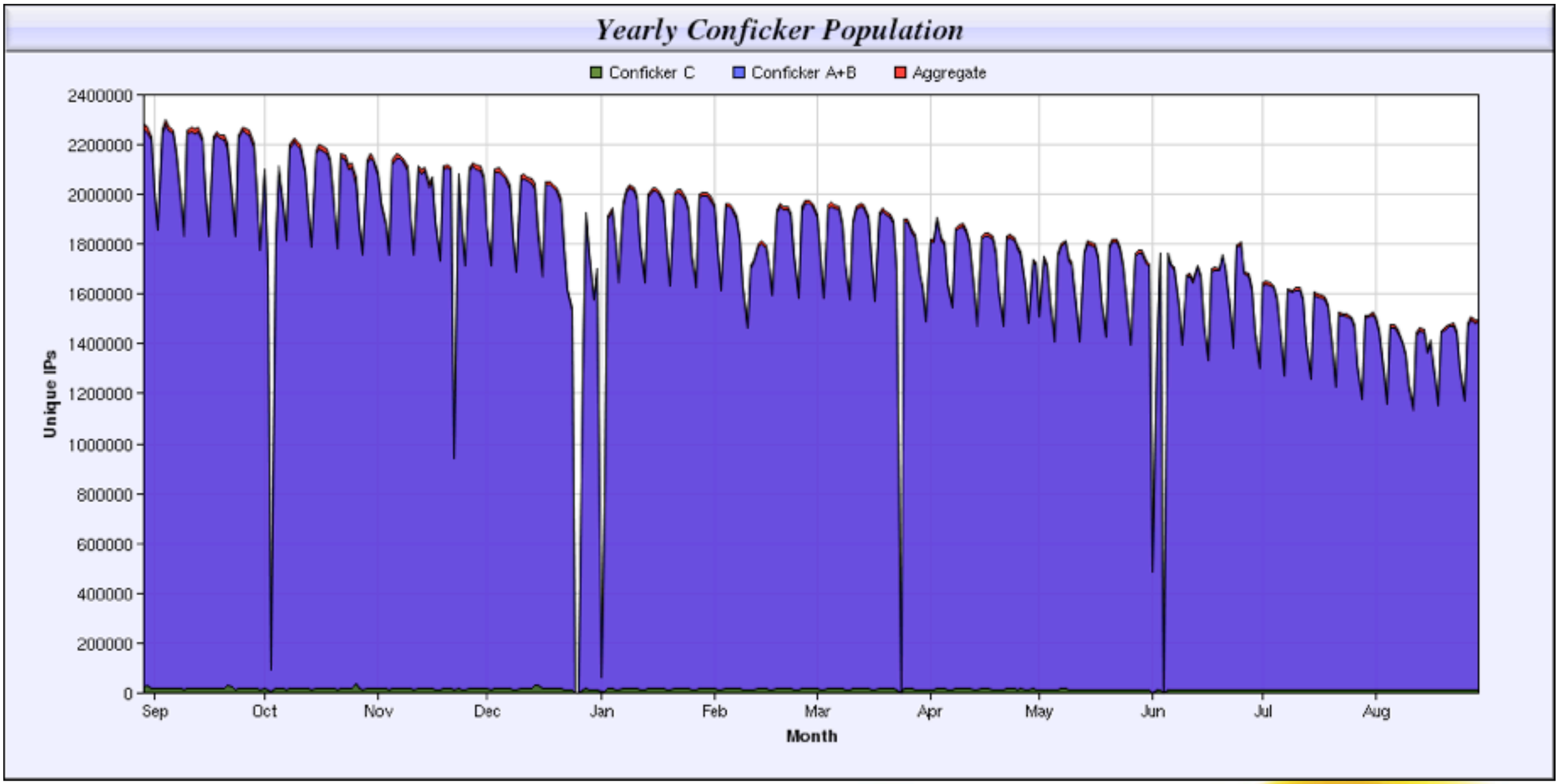
- Botnets don't need to be sophisticated
- Conficker is circulating despite the vulnerability being patched in 2008 (MS08-67)
- Zeus, released in 2007, is still a popular Trojan

- You can worry about your cyber-ninja-APT-stuxnet-wielding adversaries if you want to...

- We're going to take a look at immediate operational threats

CONFICKER

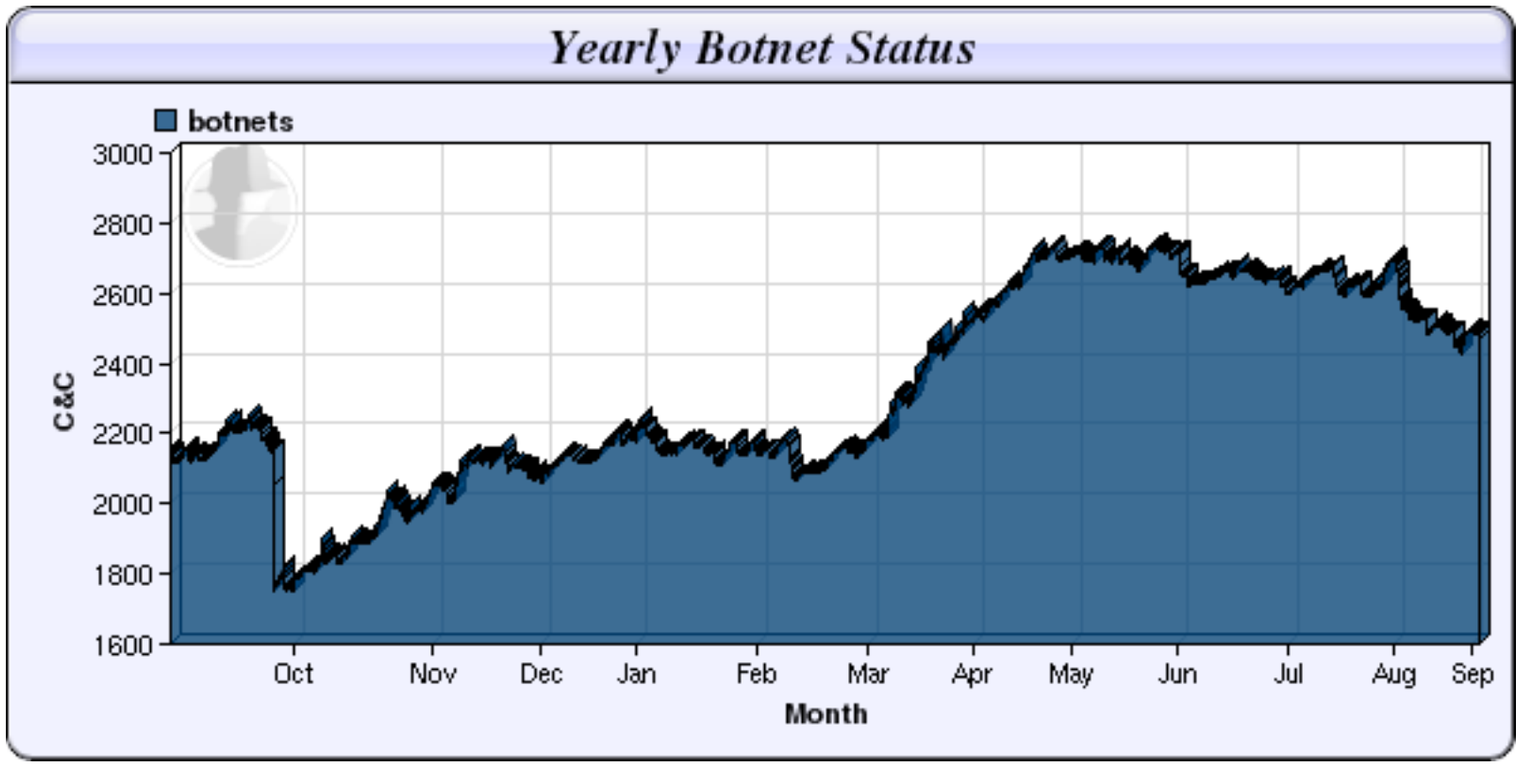
janet



@JanetCSIRT

BOTNETS

janet



@JanetCSIRT

IDS

IDS

janet

- Most botnets communicate using known and predicable protocols
- Commonly detectable using an IDS such as snort
  (ignoring encryption, clever P2P stuff, tor...)

- Can work really well using a small and select number of signatures

@JanetCSIRT

DIFFICULTIES

janet

- Easy to implement at 1Gbps
- 10Gb/s+ and it starts to get interesting
  - Snort implementation on an FPGA
  - ‘Intelligent’, filtering network taps
- Starts to get expensive, doesn’t scale

- I’ve no idea what happens at 100Gb/s, ludicrously expensive?

@JanetCSIRT

BAD BITS

janet

- Some organisations/agencies/states extend this to full ingress/egress packet capture
- Using terms like DPI wouldn't be very popular with customers!

@JanetCSIRT

NETFLOW

NETFLOW

janet

- Move away from complete packets and look only at L3 meta-data

- Our routers already (mostly) do this
- Two good open source tool-chains already exist (nfdump, flow-tools)
- COTs analysis solutions also exist

- Vastly less data to process, fewer management issues

@JanetCSIRT

NETFLOW

janet

- (relatively) cheaper
- Fewer legal and ethical issues than DPI

@JanetCSIRT

USING NETFLOW CONS

janet

- Not all routers do netflow well
- Open source tools aren't user friendly
- COTS solutions that we've looked at don't really work for us
- Netflow will be sampled
- The limitations of L3 meta-data aren't widely understood

EXPECTATIONS

janet

Not going to be as thorough as an IDS...

- Not everything is detectable using L3 meta-data alone
- Your netflow will be sampled, you'll miss things

But what can we do that's cheap, and easy to achieve using what we have?

TOOLS

janet

nfdump - actively maintained software, with tcpdump like interfaces

nfsen - graphical front end to nfdump tools, netflow based mrtg

http://nfdump.sourceforge.net/

flow-tools - an older software package, no longer maintained, doesn't support v9/IPFIX

http://www.splintered.net/sw/flow-tools/

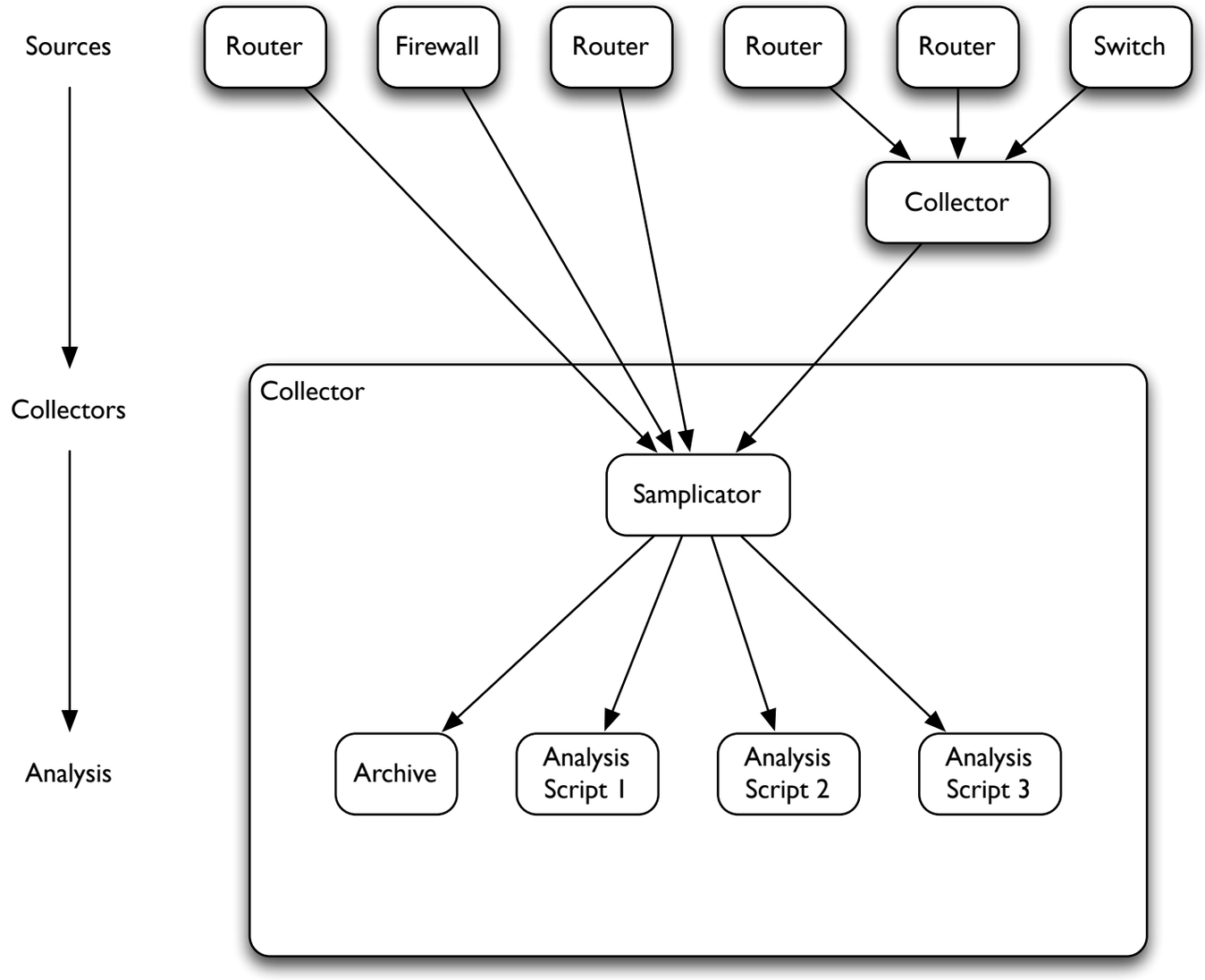
samplicator - UDP multiplexor and tweaking program

http://code.google.com/p/samplicator/

@JanetCSIRT

ARCHITECTURE

janet



@JanetCSIRT

ARCHIVING

janet

Use native nfcapd, flow-capture for storage:

- Simple, cheap, fast
- Slow to query (may be acceptable)

Use a database for storage:

- Flexible, indexing possible
- Queries can be much faster and more complex
- More intensive, more expensive

Future: maybe try something like Hadoop?

@JanetCSIRT

FILTERING

janet

Where botnet activity can be identified in a single flow, filters work well

```
$ nfdump -q -a -r $filename -o csv (dst ip a.b.c.d or dst ip e.f.g.h or ...) and dst
    port 80
```

Wrap that up in some scripts...

You can build dynamic filters, sourcing bad IP addresses from external sources:

https://zeustracker.abuse.ch/rss.php

http://rss.phishtank.com/rss/asn/?asn=786

DATABASE

janet

- Some activity is detected by reference to other flows
- Port scans by referencing SYN flows from a:x -> b:22 against SYN+ACK flows from b:22 -> a:x
- Or a connection from a:x -> b:3306 followed by scanning from b for 3306/tcp

@JanetCSIRT

RESULTS

@JanetCSIRT

CONFICKER

janet

- We can offer near-realtime detection and reporting of conficker to customers

  ... although most customers don't want this

- On 6th September there were:

  - 13 unique Janet IP addresses infected
  - 3rd largest address space in the UK
  - 37th most infected AS in the UK

- Source:
  http://shadowserver.org
  http://bgp.potaroo.net/as2.0/bgp-originas.txt
-

FORENSICS

janet

- If a compromised host had connections from a.b.c.d, we can now find out what else on Janet they've been connecting to in recent days

- Can be incredibly valuable: we've seen a very well targeted spammer subsequently log into webmail.foo.ac.uk with legitimate credentials a few hours after the attack

CERT NEWS

CISP

janet

CISP - Cyber Security Information Sharing Partnership

http://www.cisp.org.uk/

Please feel free to contact me if you need a reference to join.

@JanetCSIRT

CERT-UK

janet

- A "National CERT" team is being formed
  - Originally announced in December 2012
  - Bring together existing .gov.uk CERT teams and expertise?
  - CISP will become part of this team

@JanetCSIRT

THANK YOU

Janet, Lumen House
Library Avenue, Harwell Oxford
Didcot, Oxfordshire
t: +44 (0) 1235 822200
f: +44 (0) 1235 822399
e: service@ja.net