REDJACK

Darkspace Construction and Maintenance

Jeff Janies and M. Patrick Collins

RedJack

FloCon 2011

What are Darkspaces?

REDJACK

- **Simple definition:** Externally routable address block(s) to which no legitimate network traffic should be destined.
  - No active hosts
- Gives us an understanding of “background radiation”.
  - Junk traffic that enters a network
  - Ex. Scanning, backscatter

Darkspaces are Found Items

REDJACK

- Blocks of unallocated addresses
  - Large networks likely have several large blocks of darkspace.
  - Most networks have dark bits interspersed through the network. *(Result of historical allocations)*
- Need consistent information
  - Estimations from 2 empty /16's should be comparable to 130,000 random dark addresses.

Darkspace Types

REDJACK

- **Dedicated:** A CIDR-block dedicated to being a darkspace
  - Never contained active hosts
- **Partially Populated:**
  - **Static Active Hosts:** Active hosts are present, but static IP addresses. (CAIDA)
  - **Roaming Hosts:** Active hosts are present and have dynamic IP addresses. (Harrop *et al.*)

Bias on the Information Source

REDJACK

- Bias may result from:
  - Misinterpretation of legitimacy of traffic
  - Over/under prediction of darkspace's traffic volumes
- Bias may cause
  - Incomparable "information"
  - Over/under estimation of "background radiation"

Improved Definition

REDJACK

- Externally **routable** address block(s) for which all traffic may be **accounted for as legitimate or illegitimate** based on observable, **consistent address allocation** and **size**.

Construction Methodology

REDJACK

- "Construction" = Selection of address blocks.
  - Rule set for what is used and how it is interpreted.

- Rules based on measurable **characteristics.**
  - Characteristics have two meanings:
    - **Observer** (us)– Must care about all.
    - **Attacker** (the motivated component of radiation) – Only can see or care about a subset.
  - Some controllable, Some based on circumstance

Darkspace maintenance

REDJACK

- Maintain predictability:
  - A) Our observer characteristics must remain the same.
  - B) Modifications must be accounted for when comparing measurements.
- Characteristics for attackers may not be controllable.
  - Exception: Honeypots ***(not discussed here!)***

Characteristics

REDJACK

- Unknown to Attackers
  - **Routing –** Who can contact it?
  - **Size –** How big is it?
- Directly impacts attackers and/or radiation
  - **History –** Does it have a past?
  - **Population –** What is in it?

Routable

REDJACK

- **Measurement:** A determination of if the address space is capable of receiving traffic without address translation or mapping.
  - Ex. 192.168.0.0/16 is not considered “routable” in this way.

- *This is a binary characteristic*
  - *If un-routable, no darkspace may be made.*

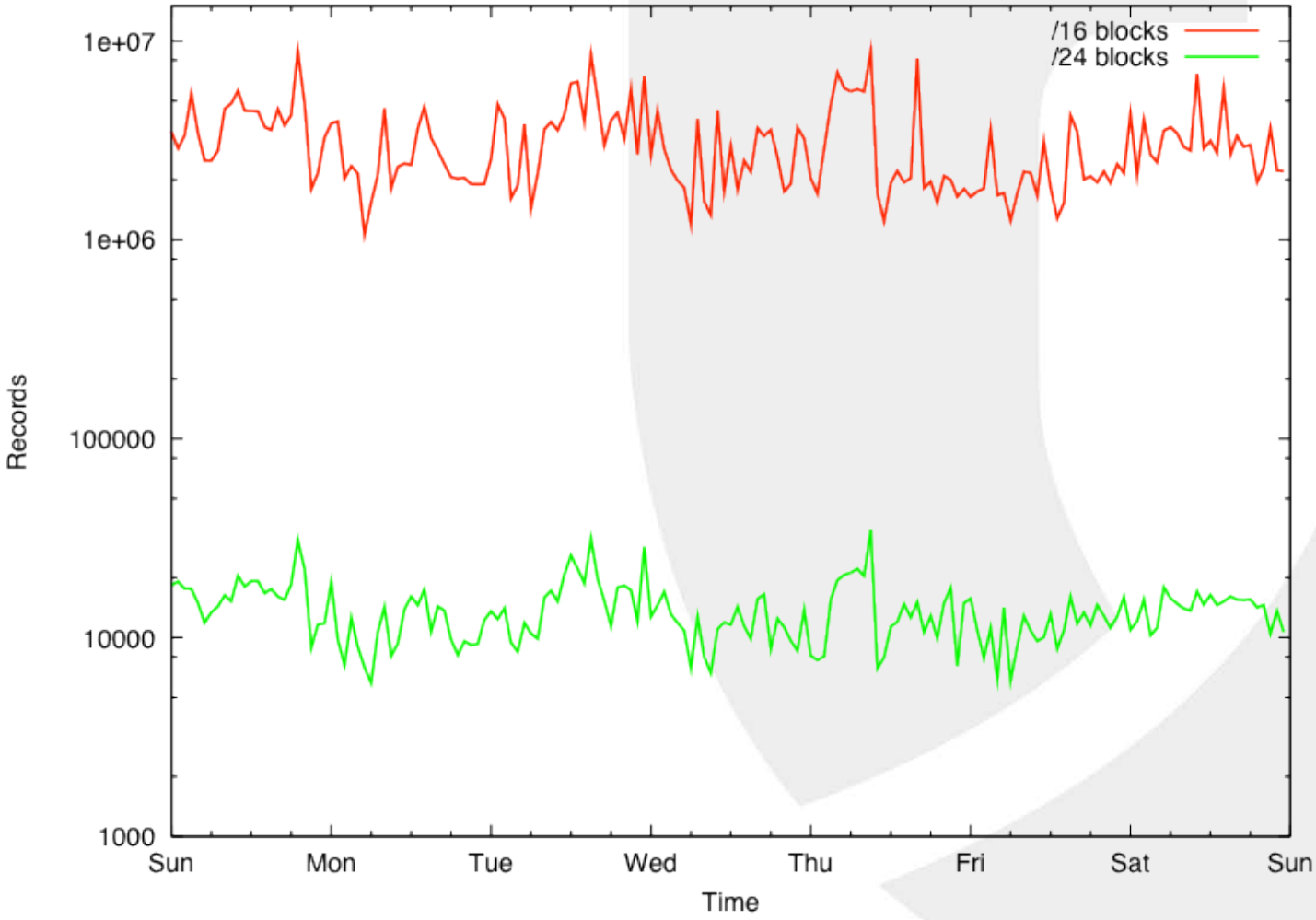
Size

REDJACK

- **Measure:** Number of available addresses for observation.
  - Effects expected volume
- Demonstration:
  - Various non-overlapping darkspaces.
  - /16 vs. /24 (sample of 100 each)
  - 1 week of traffic

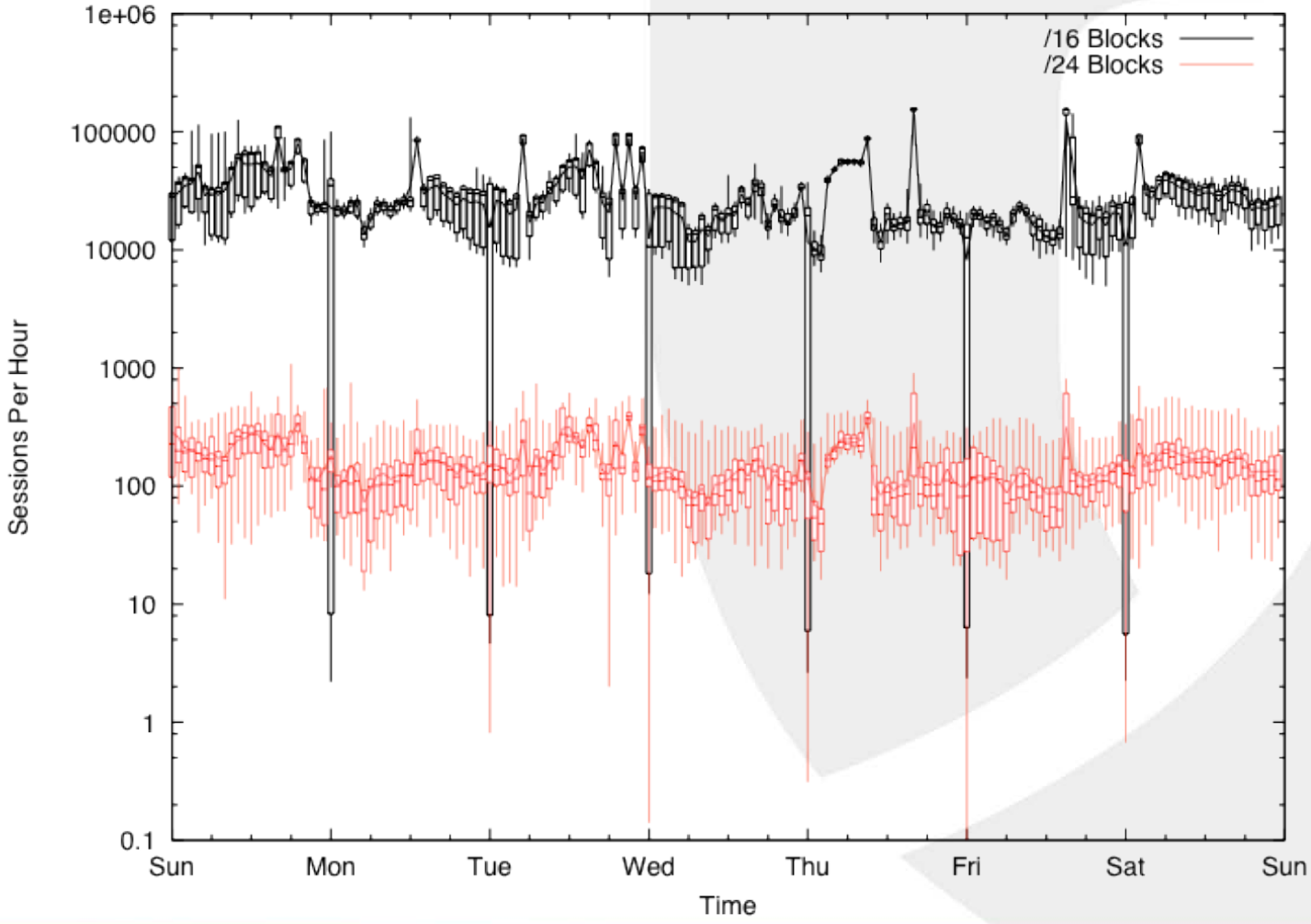
All Records

REDJACK



Record Counts Per Hour

REDJACK



History

REDJACK

- **Measurement:** The stability of light and dark addresses in a block over time.
  - Causes incorrect interpretations of activity

- Probability of receiving a scan
  - In an ideal world, $P(x) \approx 1/N$, where N is the total number of hosts
  - History can change this, even if only one host was previously active!

History

REDJACK

- Experiment:
  - Examined 2 non-consecutive weeks of traffic.
  - Take 50 IP addresses observed as dark for both.
  - Add IP that was lit in the first week and dark in the second.

- The partially lit IP received >90% of the traffic to the 51 addresses in the second week!

Population

REDJACK

- **Measurement:** The number of “active” hosts in a darkspace.
- Do attackers have an interest in netblocks only if:
  - X hosts are active
  - The netblock is announced active
  - Or, they don’t care at all and hit everything equally

Population And Filtering

REDJACK

- Population isn't just a matter of active hosts.
  - Scans for vulnerable hosts:
    - Network without vulnerability are seen by scanner as "dark".
    - What use is a /24 of Amigas?
- What's the "dark factor" on light spaces
  - If you toss out payload bearing sessions, are dark and light networks identically hit?

Characteristics of Construction

REDJACK

	Routable	Size	History	Population
Dedicated	Assumed	Predictable	Predictable	Controllable
Static Active Hosts	Assumed	Predictable	Predictable	Controllable
Dynamic Active Hosts	Assumed	Unpredictable	Unmanageable	Uncontrollable

If we don't know when, where or how many hosts will be active, we can't predict observations or attacker interest.

Conclusion

REDJACK

- Darkspaces should be constructed with consistency in mind.
- Characteristics for construction should include:
  - routable, size, population and history
- Dynamic active hosts have no place in darkspaces!

References

- W. Harrop and G. Armitage. Dening and evaluating greynets (sparse darknets). In LCN'05: Proceedings of the IEEE Conference on Local Computer Networks 30th Anniversary, pages 344{350, Washington, DC, USA, 2005. IEEE Computer Society.
- CAIDA. UCSD network telescope, April 2005. http://www.caida.org/data/passive/network telescope.xml.
- M. Bailey, E. Cooke, F. Jahanian, N. Provos, K. Rosaen, and D. Watson. Data reduction for the scalable automated analysis of distributed darknet trac. In IMC'05: Proceedings of the USENIX/ACM Internet Measurement Conference, 2005.