Lessons learned:

Sinkholing the Zeroaccess botnet

Ross Gibb

Attack Investigations Team
Symantec Security Response

Agenda

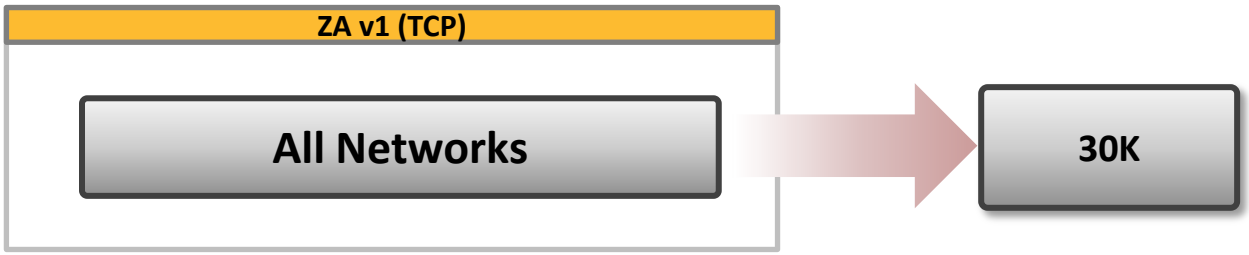
1. Introduction to Zeroaccess
2. Details of the P2P protocol
3. The sinkhole operation
4. Results of the sinkhole operation
5. Next steps

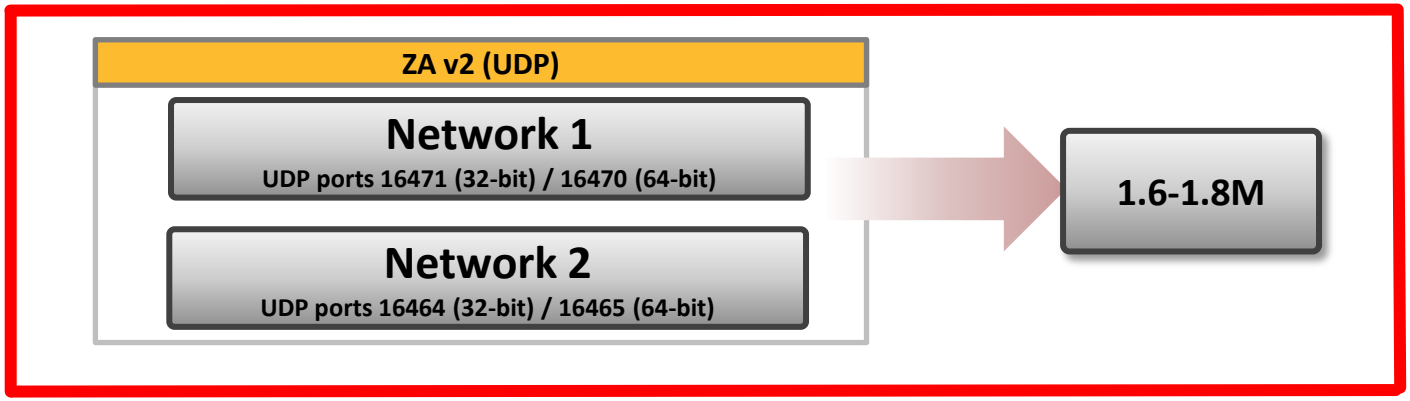
Zeroaccess (ZA) – Introduction

- Zeroaccess is a botnet, also known as ‘Sirefef’ or ‘ZAccess’ or ‘Zerokit’
- First appeared in Summer 2011
- Two major versions
  - Version 1, rootkit, TCP P2P (2011)
  - Version 2, user mode, UDP P2P (2012)
- Infected computers exclusively use the peer-to-peer (P2P) network to distribute payloads
- Can be thought of as a framework to load any module/malware
- Infection vectors include social engineering, exploit kits, and other downloaders
- Pay Per Install (PPI) and revenue sharing model
- Primary revenue is through click-fraud
- Malicious payloads use their own C&C infrastructure

ZA – Size

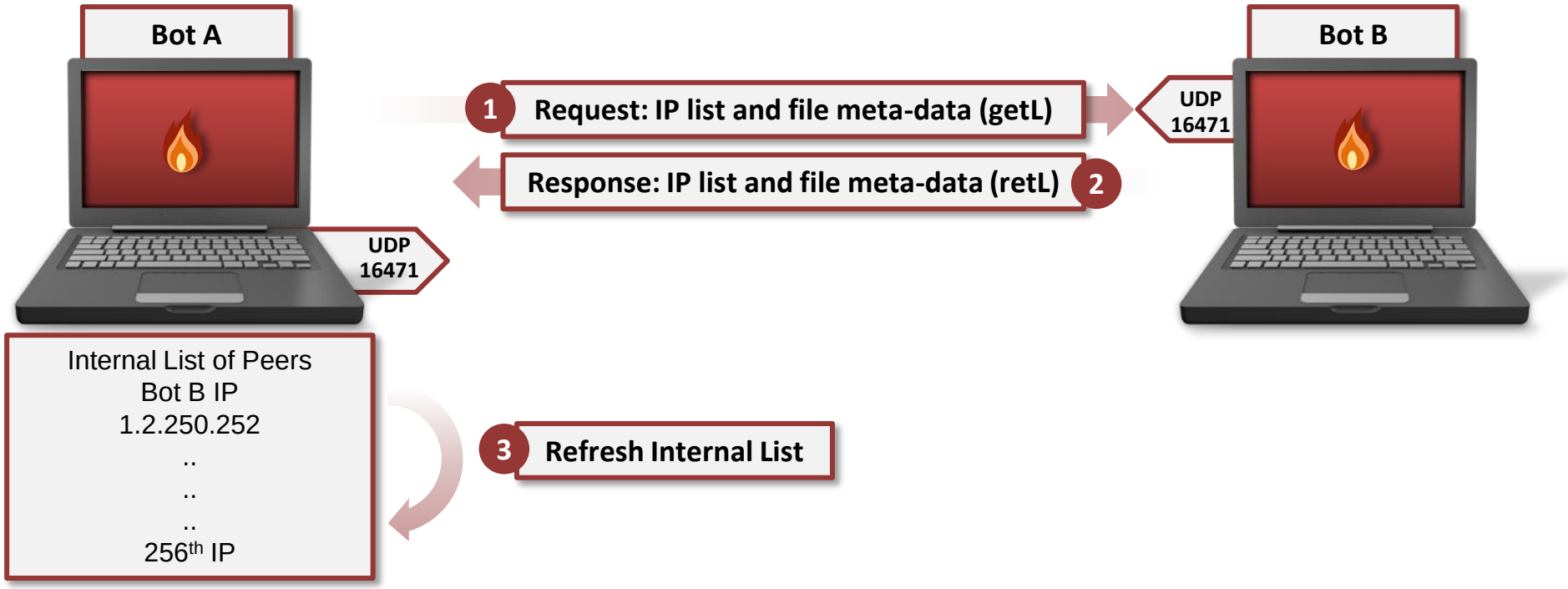
- Counts are of average daily unique infected hosts, measured in May 2013
- Networks are subdivided into 32-bit and 64-bit client networks; no inter-network / cross-port communication



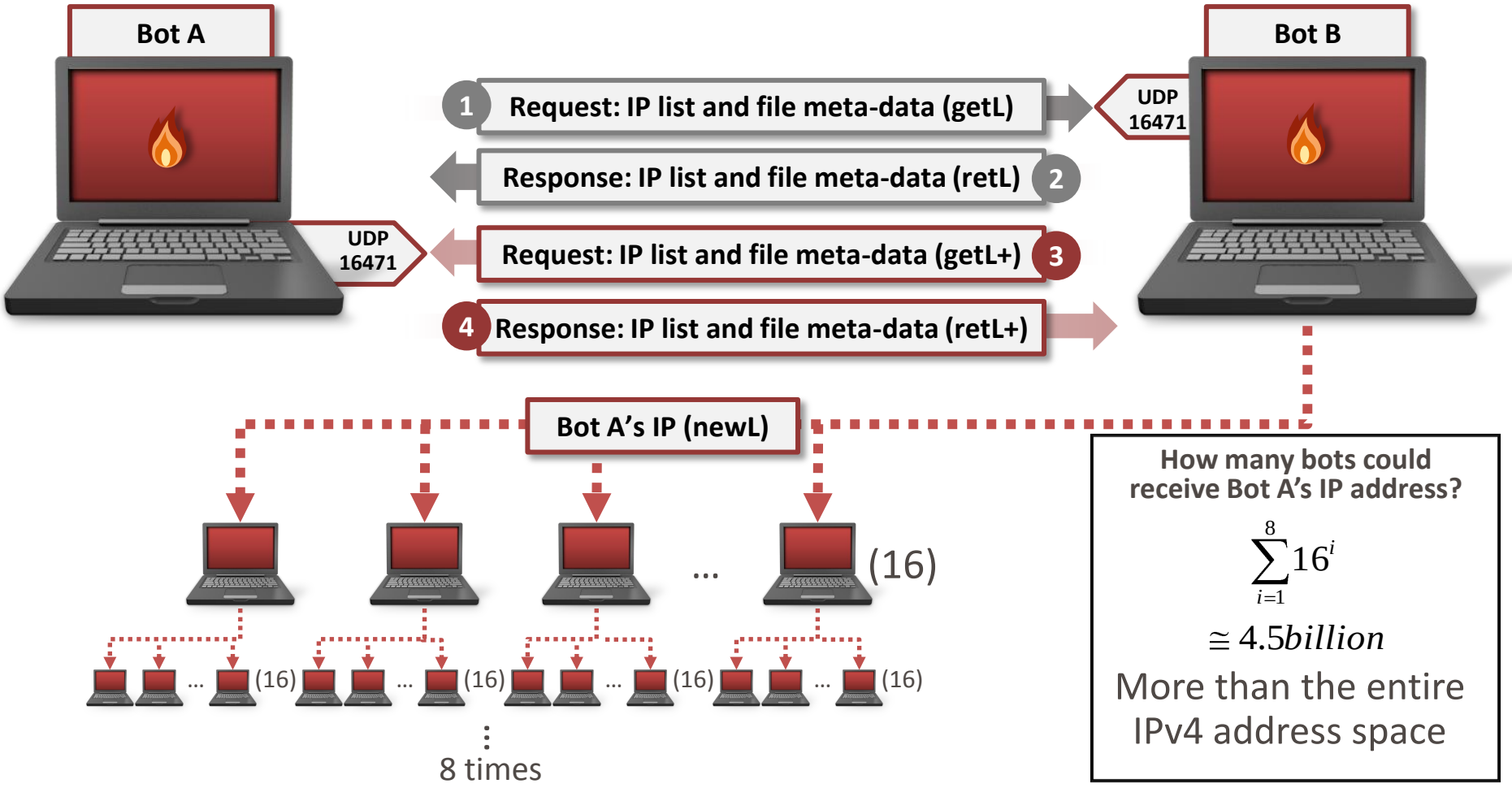


What would a sinkhole of Zeroaccess look like?

ZA – P2P Operation



ZA – P2P Operation



How many bots could receive Bot A's IP address?

$$\sum_{i=1}^{8} 16^i$$

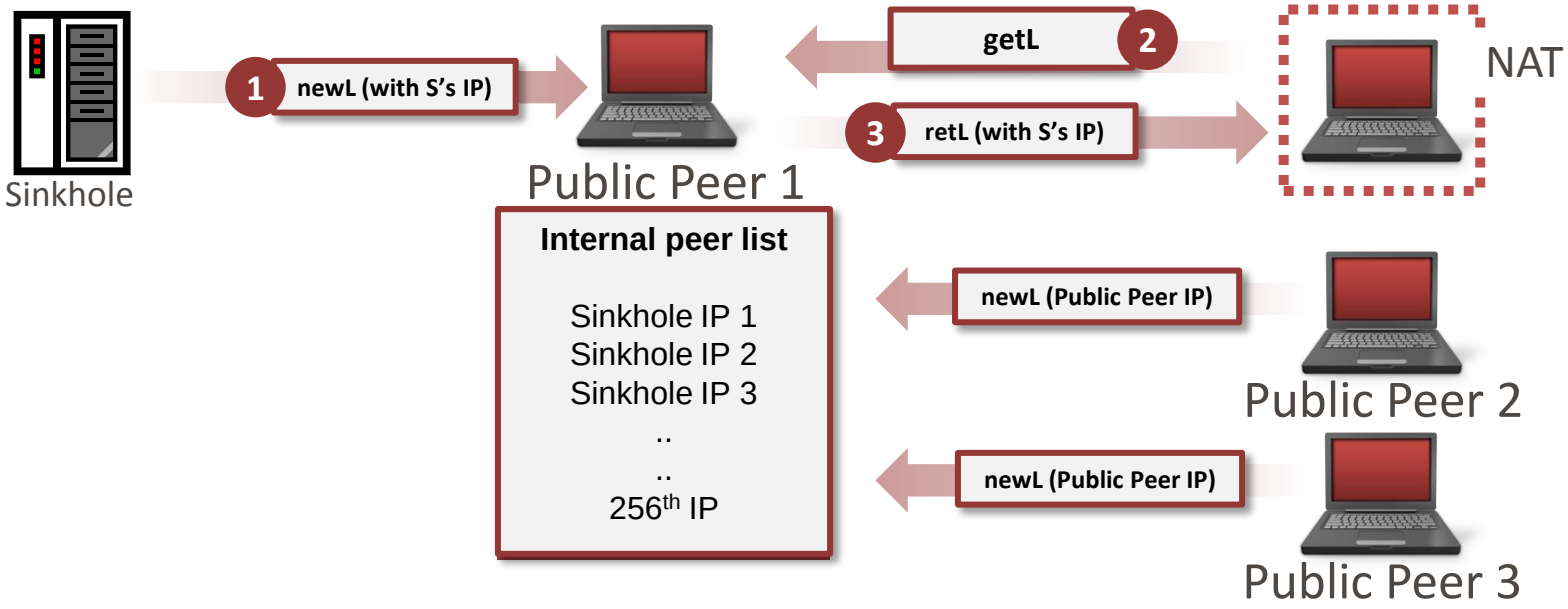
$$\cong 4.5 billion$$

More than the entire IPv4 address space

ZA – Could the P2P network be sinkholed?

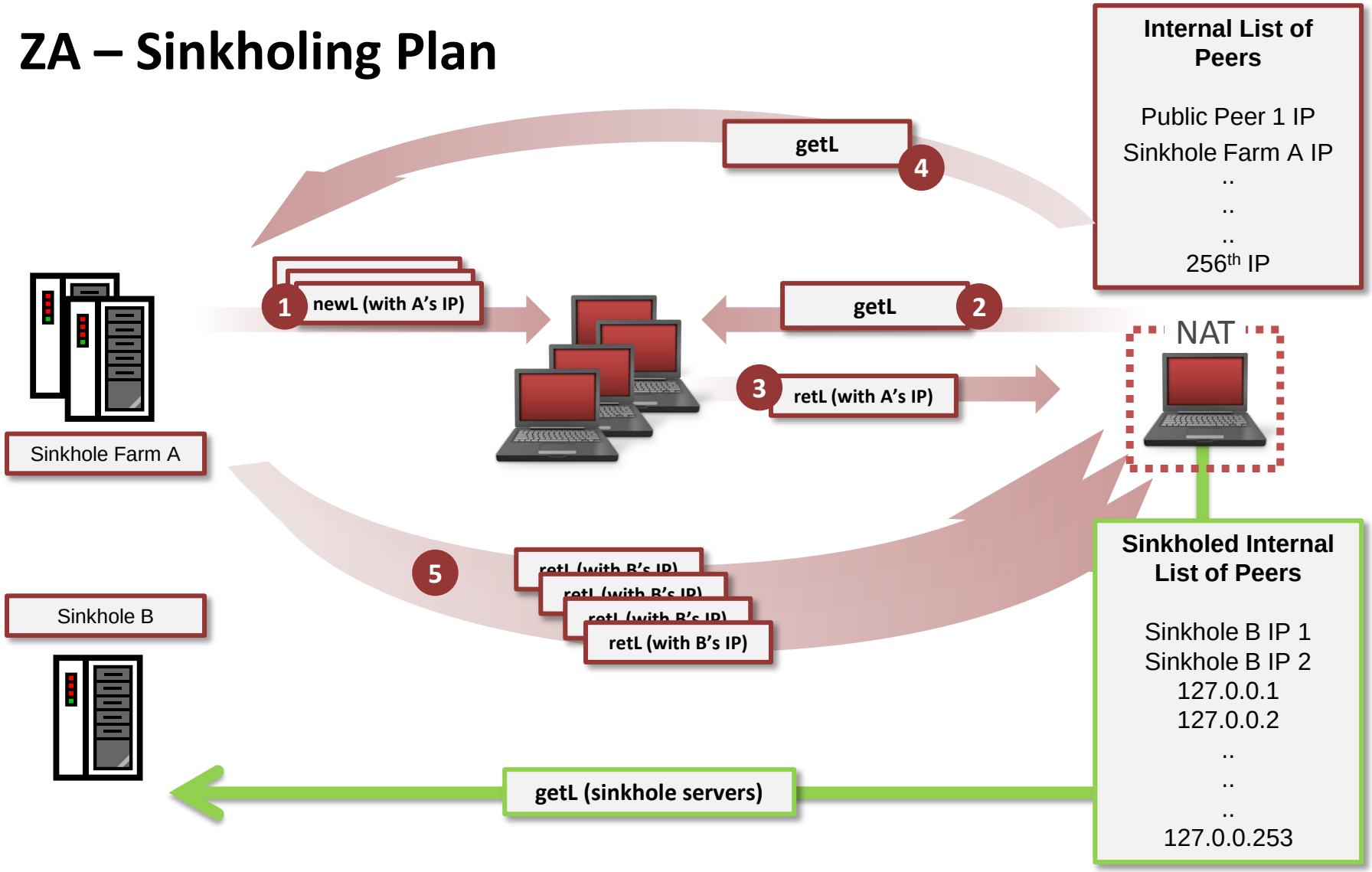
- Identified weaknesses
  - Relatively small fixed length internal peer list (256 IPs)
  - Unsolicited P2P messages are accepted from any IP
  - IP list in P2P messages is not digitally signed, only payload file meta data is digitally signed
  - Any IP address can be introduced into a remote peer's internal peer list

ZA – Challenges to sinkholing



- Takes a very large amount of continuous bandwidth
- IP churn makes it difficult to know all the public peers (super nodes)
- Zeroaccess author could use newL's in the same way to retake public peers
- Difficult to run in a network simulation prior to deployment

ZA – Sinkholing Plan

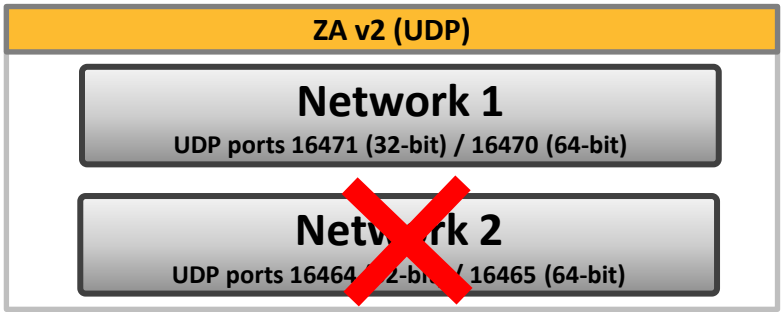


ZA – The sinkhole master plan

- Preconditions to launching the sinkhole operation
  - Simulate infected peers to understand runtime behaviour
  - Test sinkholing infected computers on a private LAN with various NAT devices
  - Test against the live P2P live as much as possible without actually sinkholing
- Expected results
  - Infected peers behind NAT devices are sinkholed and the payloads can no longer be updated
  - All infected machines can be identified for remediation

ZA – “The best laid plans of mice and men…”

- From April to June 2013, the simulation and testing of the sinkhole plan progressed
- On **June 29, 2013**, new P2P code was distributed to Zeroaccess version 2 network 2

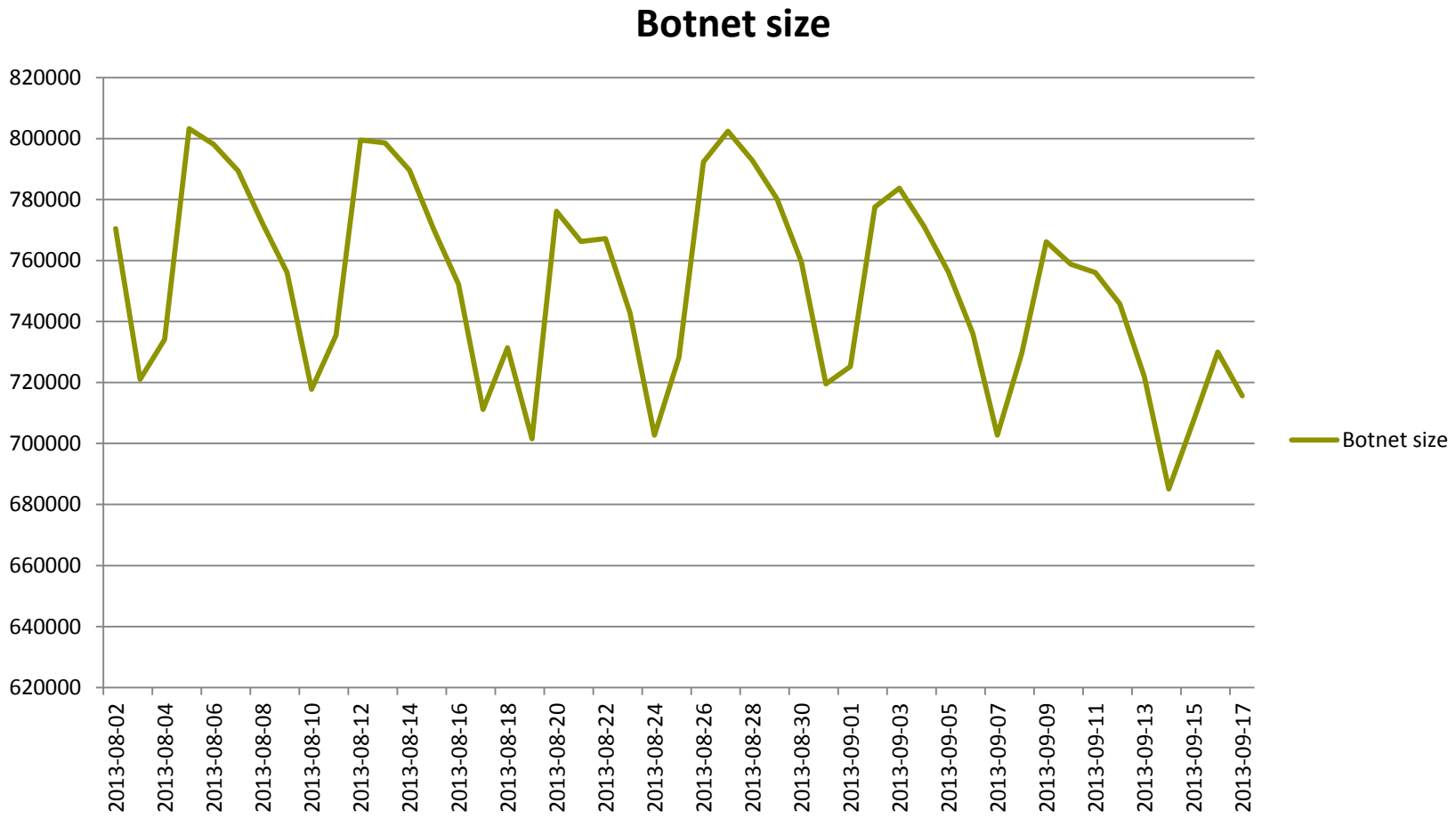


- The update made P2P Network 2 much more resilient to sinkholing
  - Reduction in instruction set (newL dropped)
  - Introduction of secondary internal peer list (holds ~16M IPs)
  - Altered run-time peer communication (secondary peer list for redundancy, and connection state table)

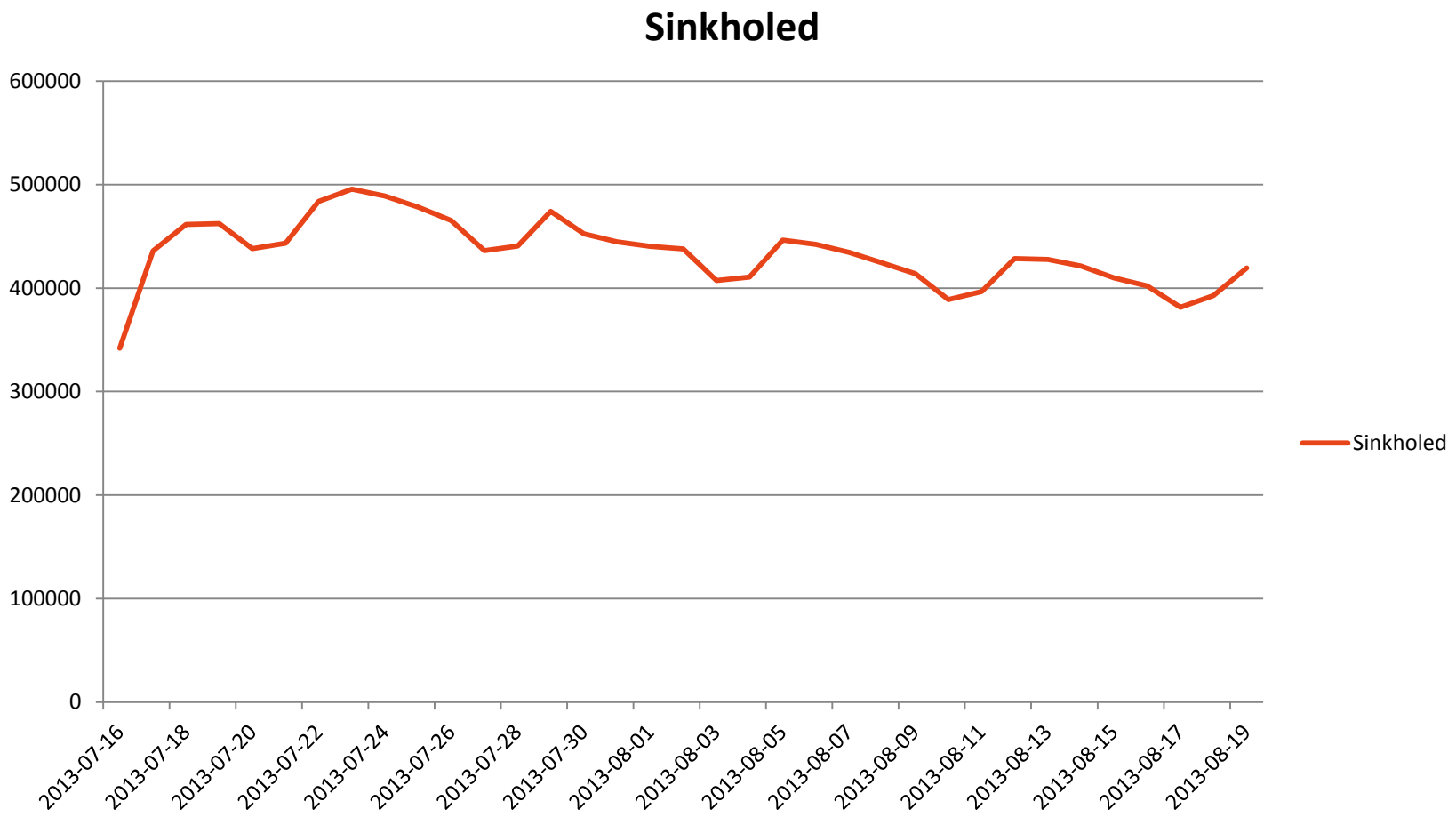
ZA – Sinkhole results

- P2P sinkhole of Network 1 initiated on **July, 15 2013**
- Available targets
  - June 29, 2013, protocol update reduced possible targets to ~900,000
- Sinkhole results week of July 17 – July 23 (in avg. daily IPs)
  - Botnet size: **797,235**
  - Number of bots sinkholed: **460,000**
  - High sinkhole count for 24 hour period **495,610**
  - Average proportion of botnet sinkholed: **58.7%**

ZA – Graph of botnet size

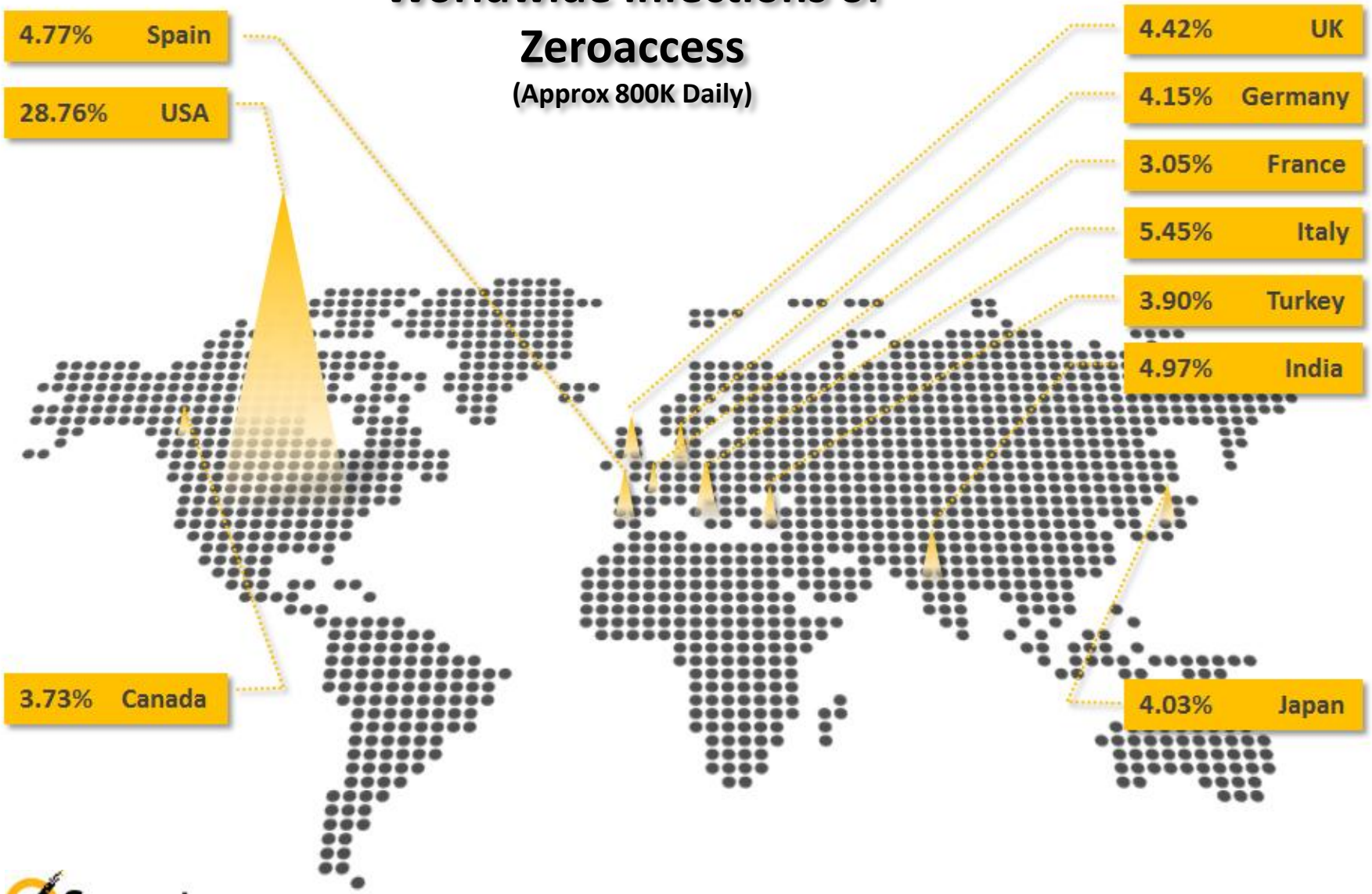


ZA – Graph of sinkhole size



Worldwide Infections of Zeroaccess

(Approx 800K Daily)



Symantec.

ZA – Next steps

- Continue to work with ISP's and CERTs to clean up infections
- Continue monitoring P2P networks (sinkholed and not), as well as payload infrastructure
- Continue with other avenues of investigation

ZA – Questions

Ross Gibb

ross_gibb@symantec.com

Attack Investigations Team (AIT)
Symantec Security Response
Culver City, California

Thank you!