WORKING TOGETHER: LE AND PRIVATE SECTOR BOTNET TAKEDOWNS

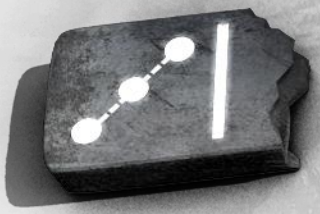
Thomas Grasso (FBI)

Alan Neville (Symantec)

Agenda

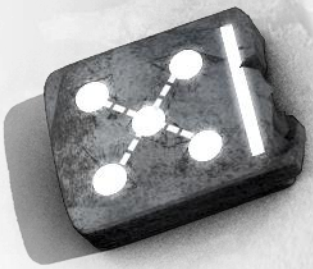
What are botnets?

Approaches to takedowns



Zeroaccess takedown

Gameover Zeus takedown



LE Involvement in takedowns

Conclusions

Q&A

What are botnets?

Growing resilience of cybercrime networks

TRADITIONAL BOTNET	PEER TO PEER BOTNET
	
Single point of failure	No single point of failure
Only one or a few C&C servers	Every peer acts as C&C server
Vulnerable to takedown & sinkholing	Difficult to take down or sinkhole

Unsurprisingly, cybercriminals are increasingly moving to P2P infrastructure

How we took out half a million ZeroAccess bots

ZeroAccess uses highly resilient P2P architecture

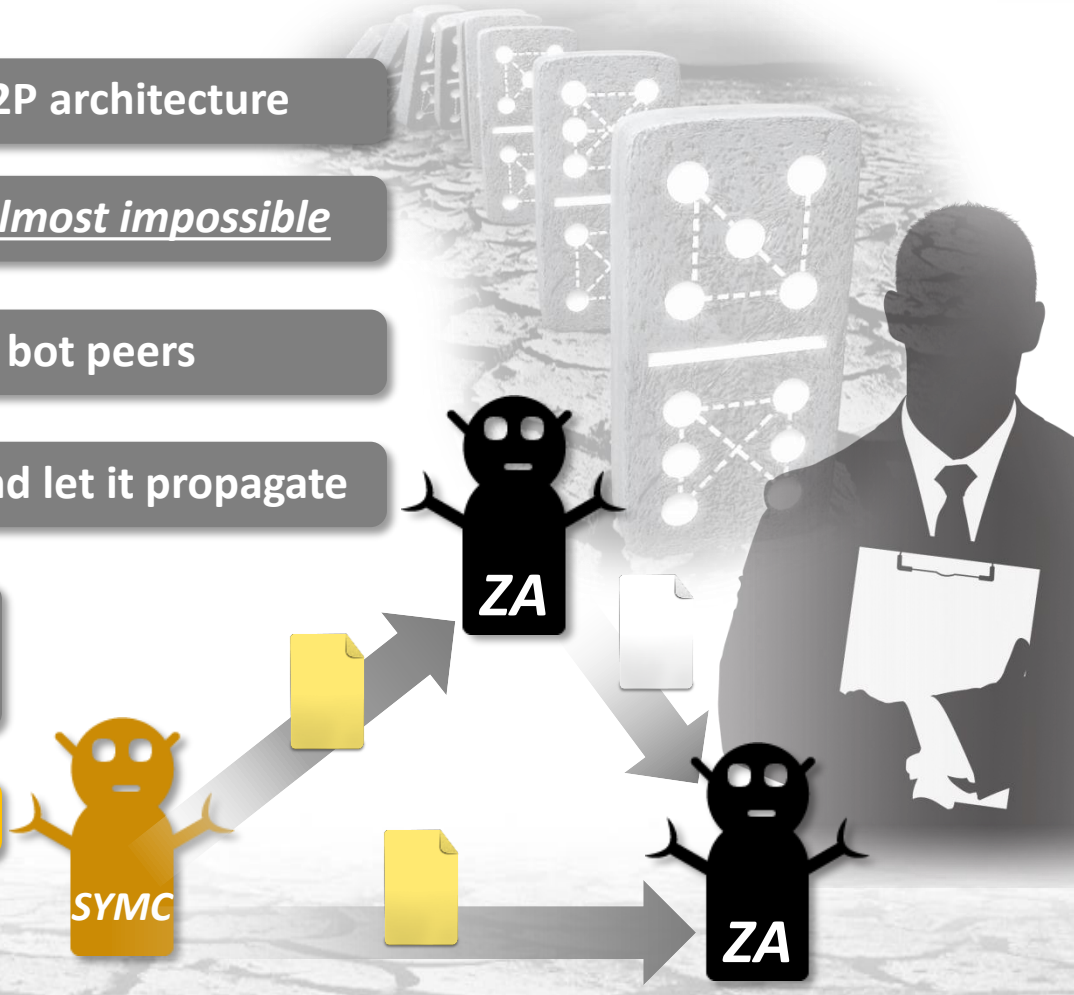
Each bot acts as a C&C, sinkholing *almost impossible*

Create sinkholes that act like bot peers

Inject sinkhole address in peer list and let it propagate

Eventually bots only have our sinkhole peer address

GAME OVER FOR ZEROACCESS!



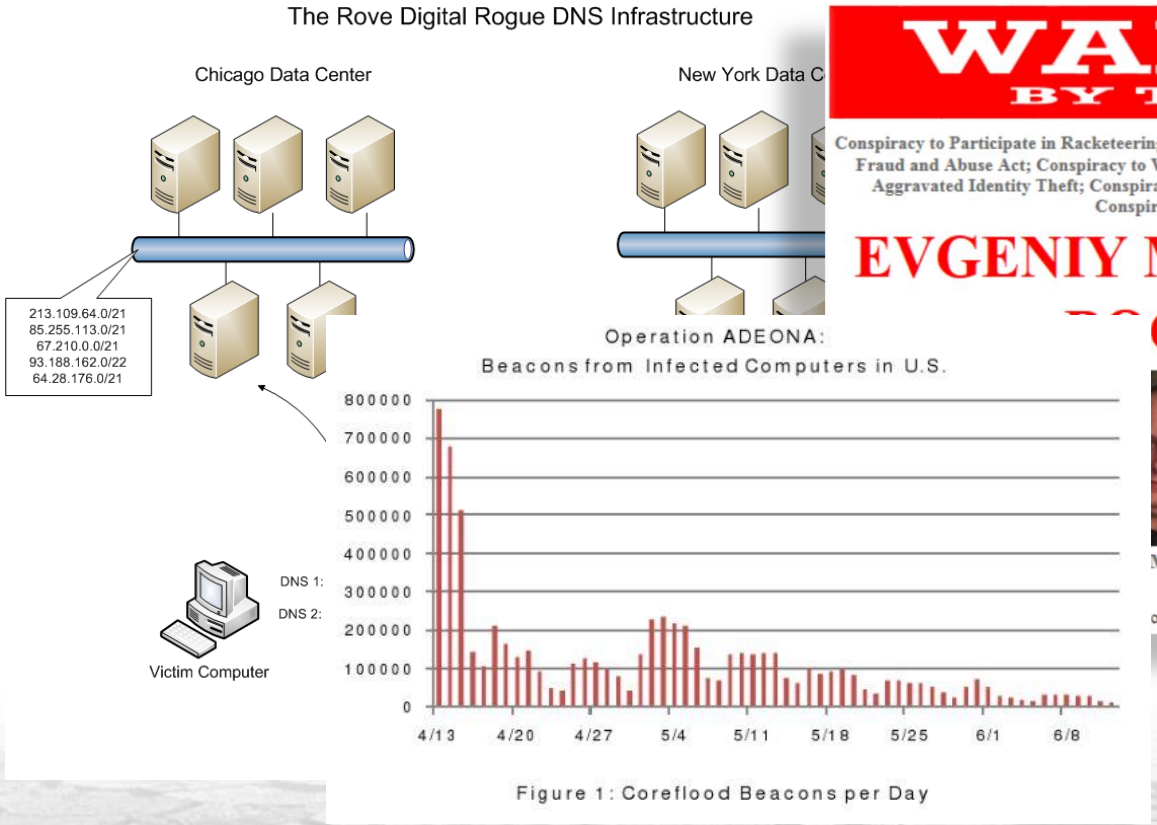
Operation Tovar:
Takedown of GameOver & Zeus/Crytolocker

COLLABORATION BETWEEN LAW ENFORCEMENT AND SECURITY INDUSTRY

Collaborative Approach to Botnet Takedowns

Botnet Threat Focus Cell

- A collaborative effort involving government, private sector and academia to combat the botnet threat.



Botnet Threat Focus Cell Approach

1. Identify and rank most serious botnet threats
2. Initiate and support investigations
3. Provide mitigation and remediation support to private sector and government
4. Reduce Botnet Threat:
    1. Remove threat actors from playing field
    2. Disable and dismantle botnets
    3. Develop countermeasures

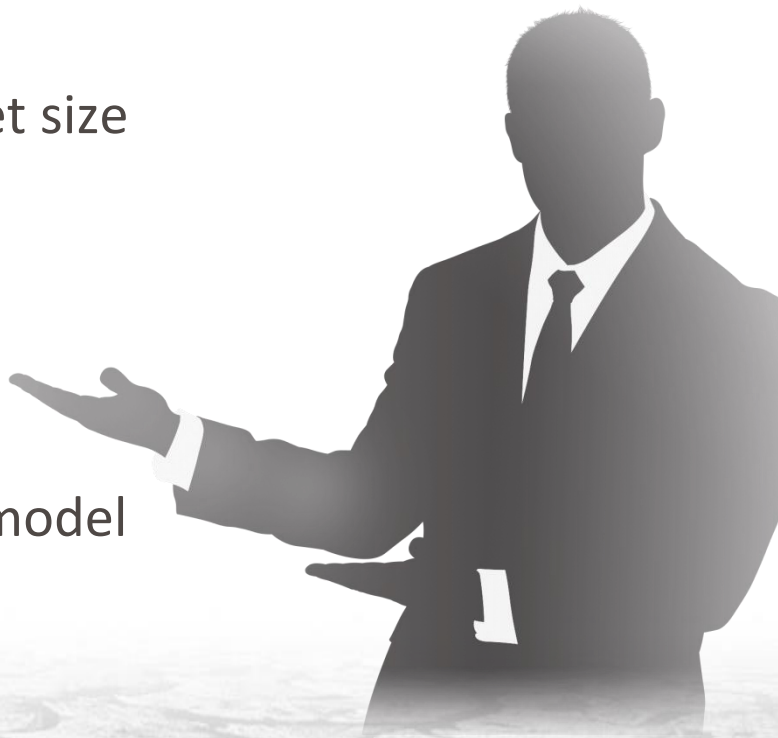
Top Ranked Botnets

Botnet	Use
Dridex	Banking/Credential Theft
Cryptolocker/Cryptowall/CTB Locker	Extortion
Zeus/Gameover Zeus	Banking/Credential Theft
Kelihos	Spam
Dyre	Banking/Credential Theft
Neverquest	Banking/Credential Theft
Angler	Exploit Kit
Dirtjumper	DDoS
Booters	DDoS

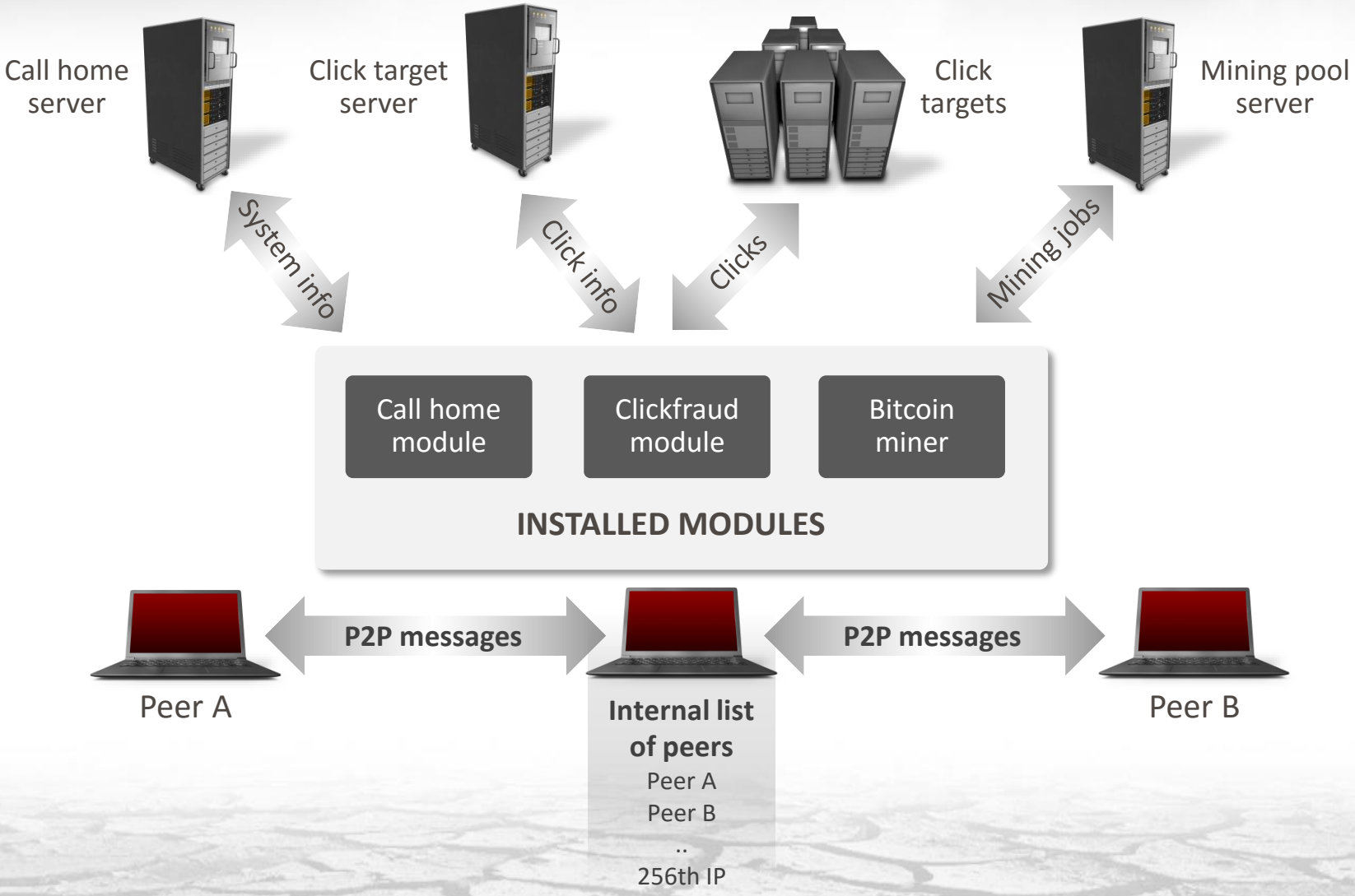
ZeroAccess takedown

Zeroaccess - Introduction

- Lucrative Trojan horse used to create a money making botnet
- Involved in cyber-crime activities
  - Bitcoin mining and click-fraud
- Technically advanced
- Widespread – estimated 1.9 million botnet size
- Infected through
  - Social engineering
  - Exploit kits
  - Other downloads
- Pay Per Install (PPI) and revenue sharing model
- Primary revenue through click-fraud

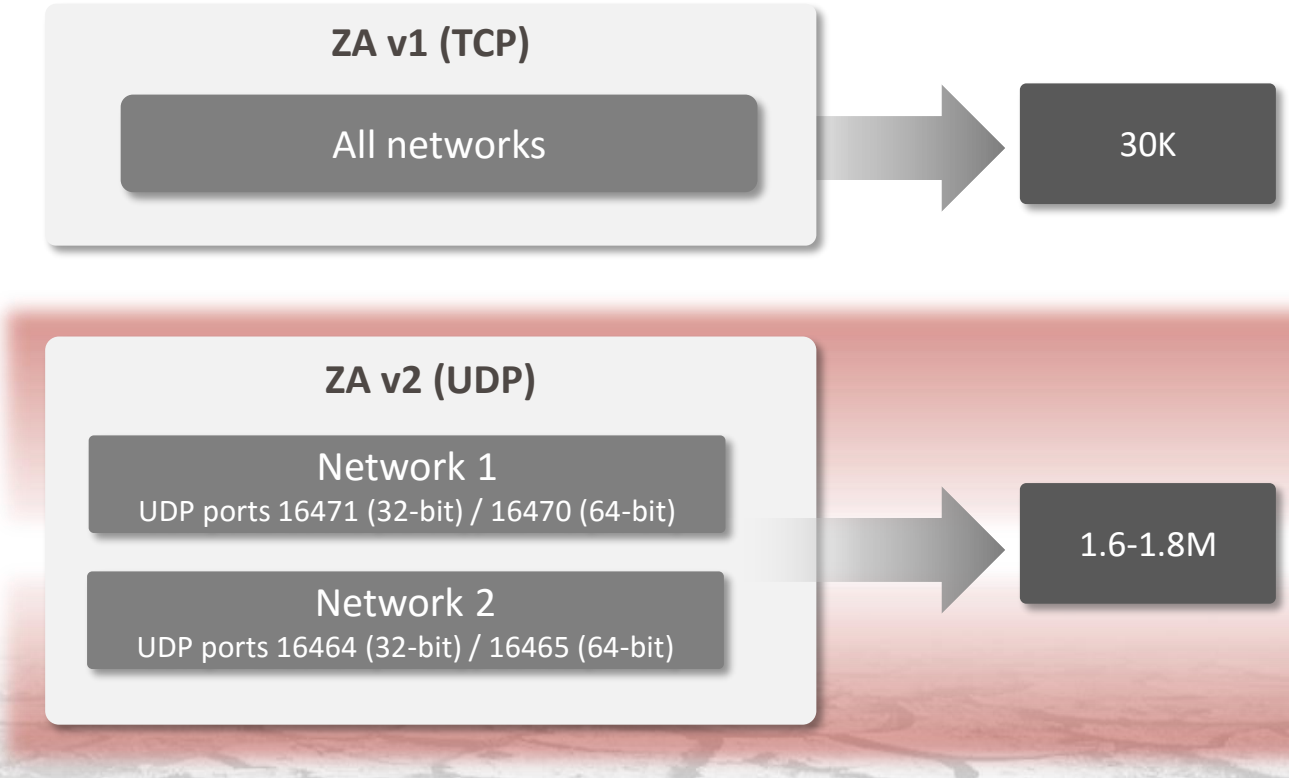


ZA – Architecture

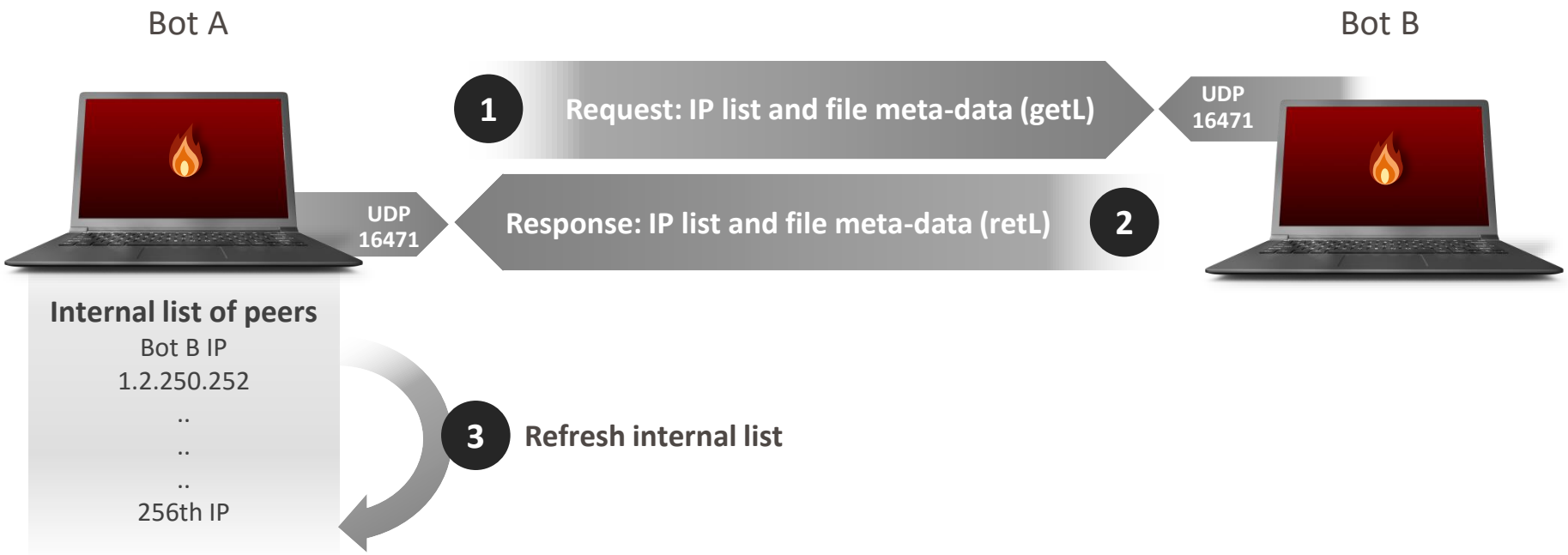


ZA – Size

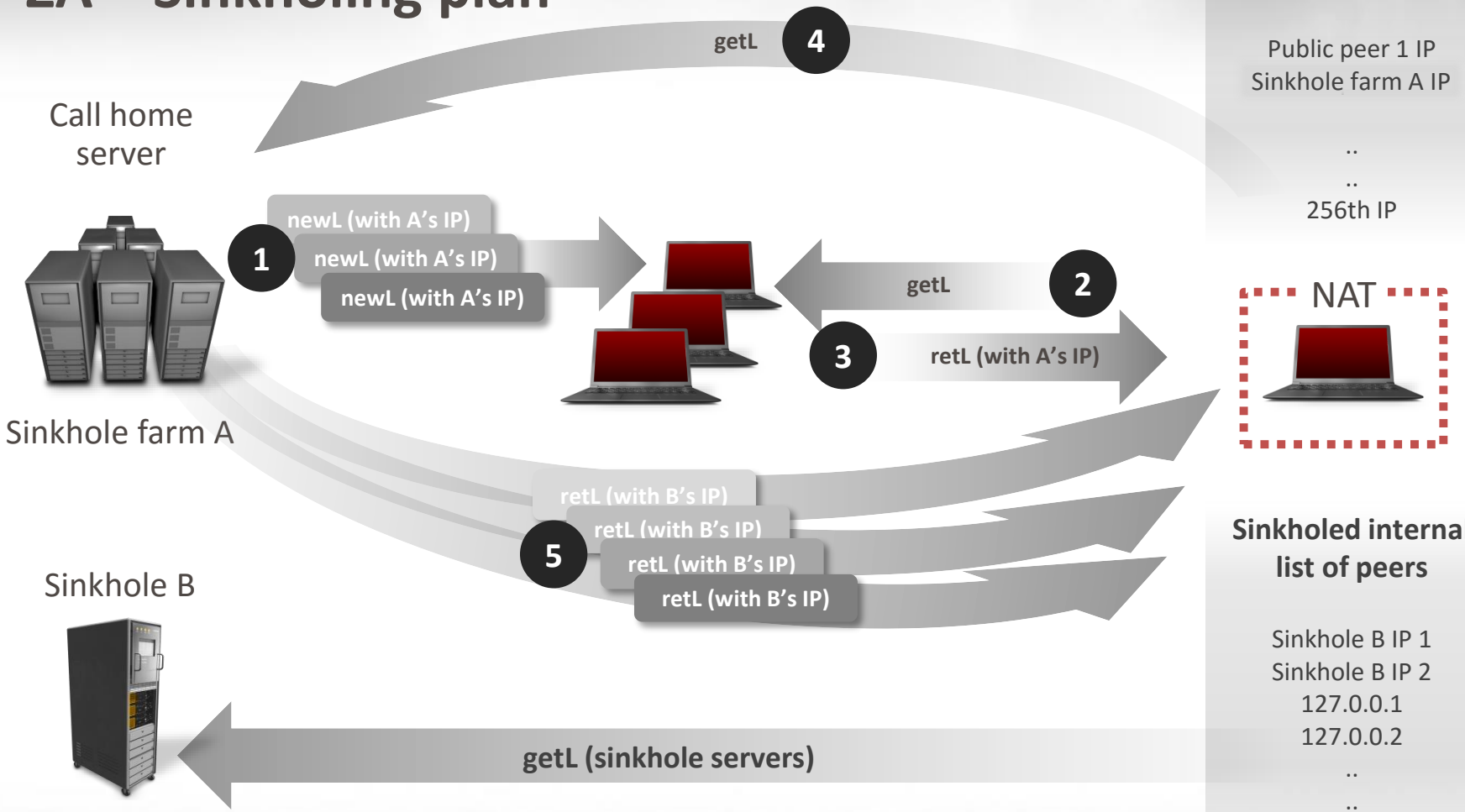
- Counts are of average daily unique infected hosts, measured in May 2013
- Networks are subdivided into 32-bit and 64-bit client networks; no inter-network / cross-port communication



ZA – P2P operation



ZA – Sinkholing plan



Internal list of peers

Public peer 1 IP
Sinkhole farm A IP

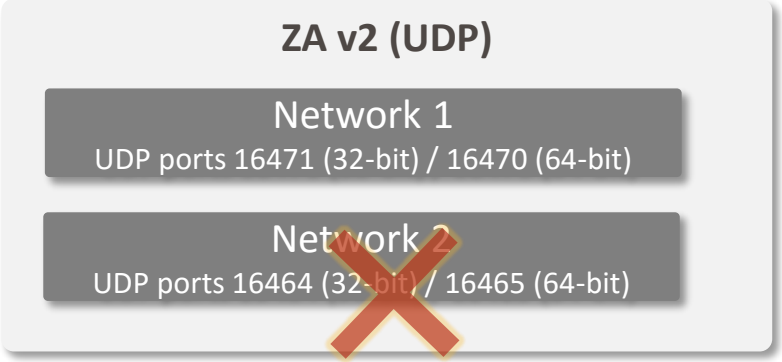
..
..
256th IP

Sinkholed internal list of peers

Sinkhole B IP 1
Sinkhole B IP 2
127.0.0.1
127.0.0.2
..
..
..
127.0.0.253

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%**

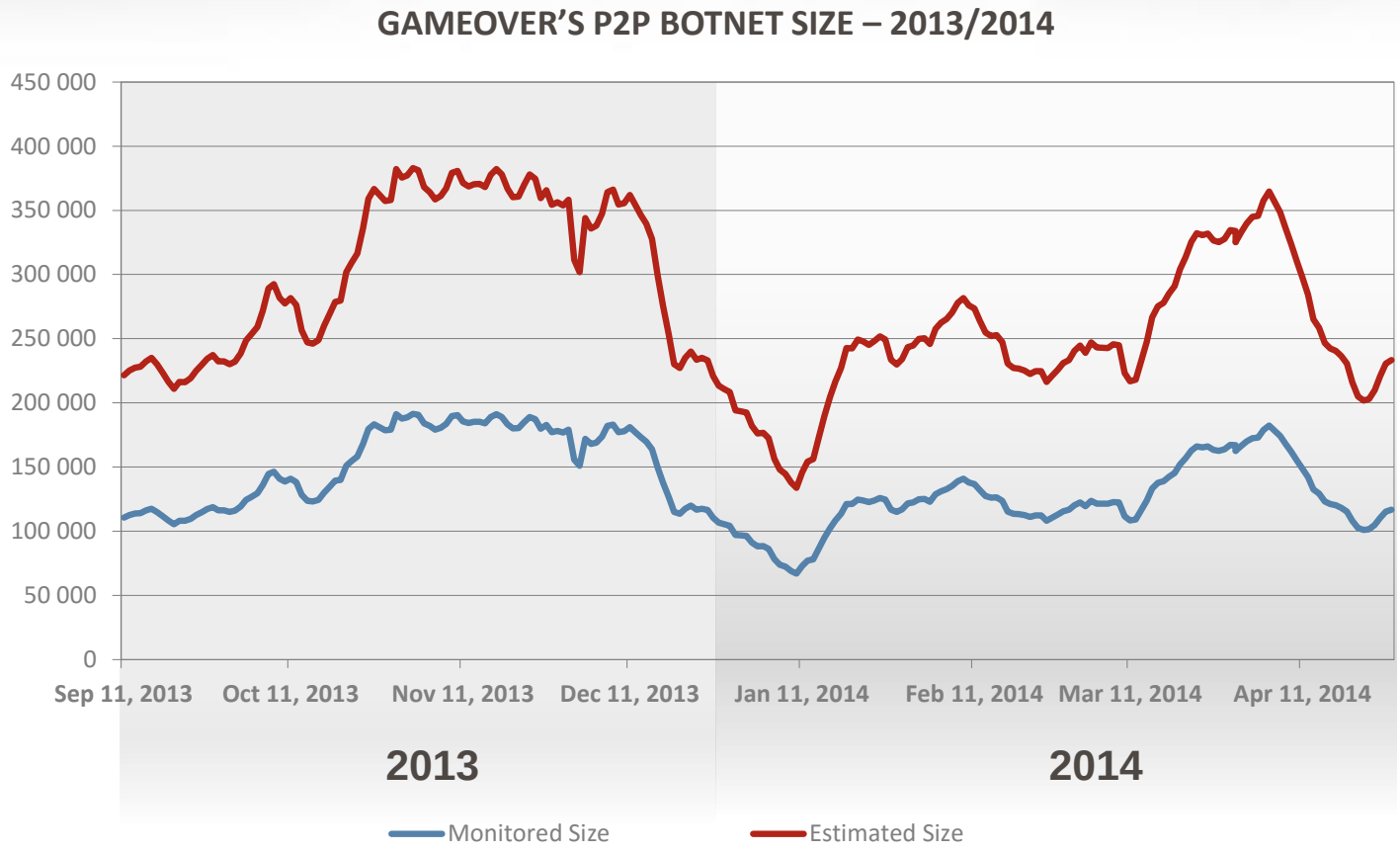
ZA – Graph of sinkhole data

Gameover Zeus Takedown

Gameover Zeus - Introduction

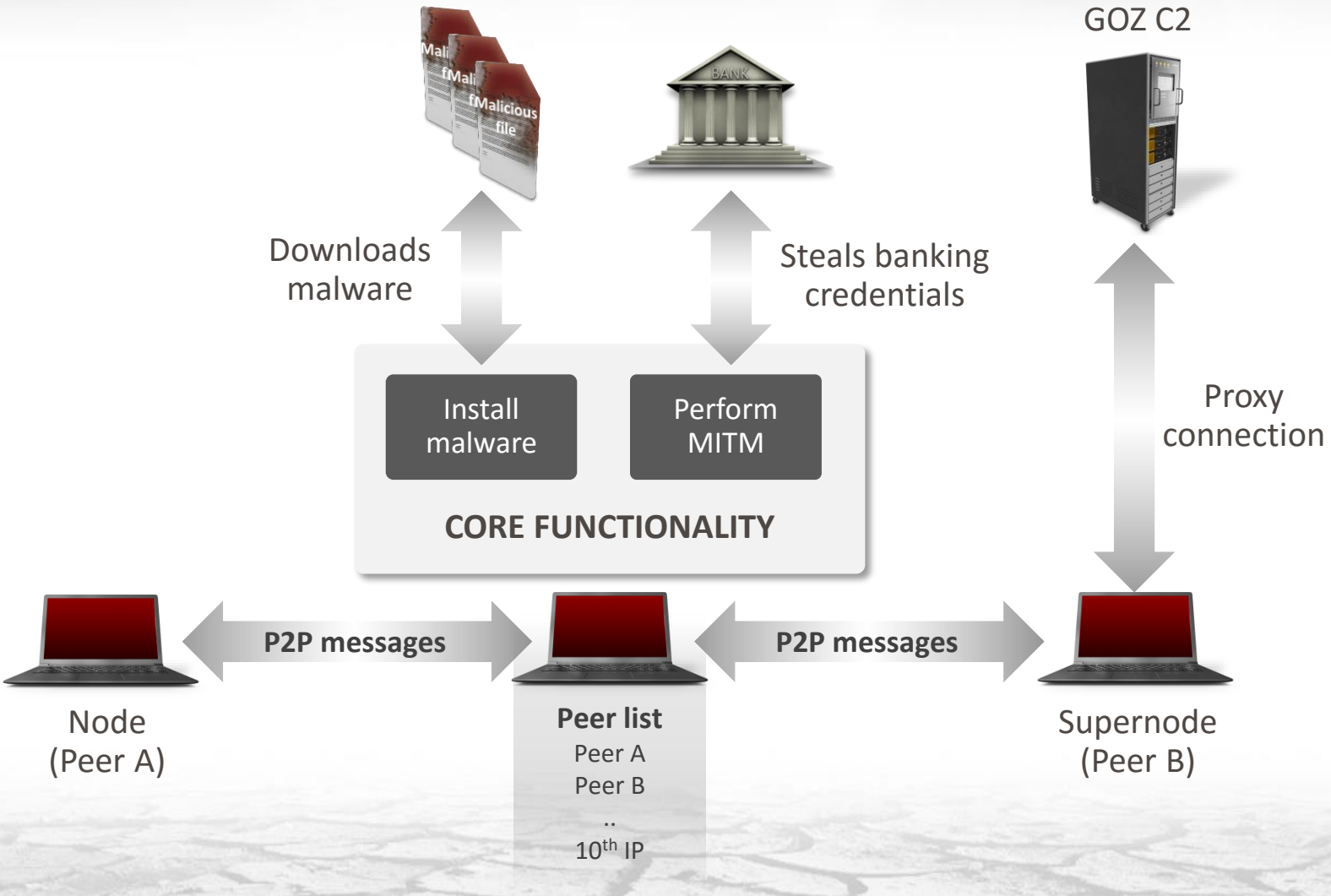
- Advanced financial fraud Trojan
- Millions of infections worldwide since its inception in 2011
- Variant of Zeus malware
  - Lots of re-working to the Zeus code base
- Command and control
  - Peer-to-peer (P2P)
  - Falls back on Domain Generation Algorithm (DGA)
- Used to download additional malware
  - Ransomware / Cryptolocker

Botnet size



The bot master has maintained a relatively steady network of hundreds of thousands of infected computers around the world.

Gameover – Architecture



Sinkhole plan

Challenges to sinkholing the P2P infrastructure

- Requires number of sinkholing servers at different providers
- Locking DGA domains
  - May not be able to guarantee sinkhole servers are up 24/7
  - Avoid risk of attackers performing DDoS against sinkholing infrastructure

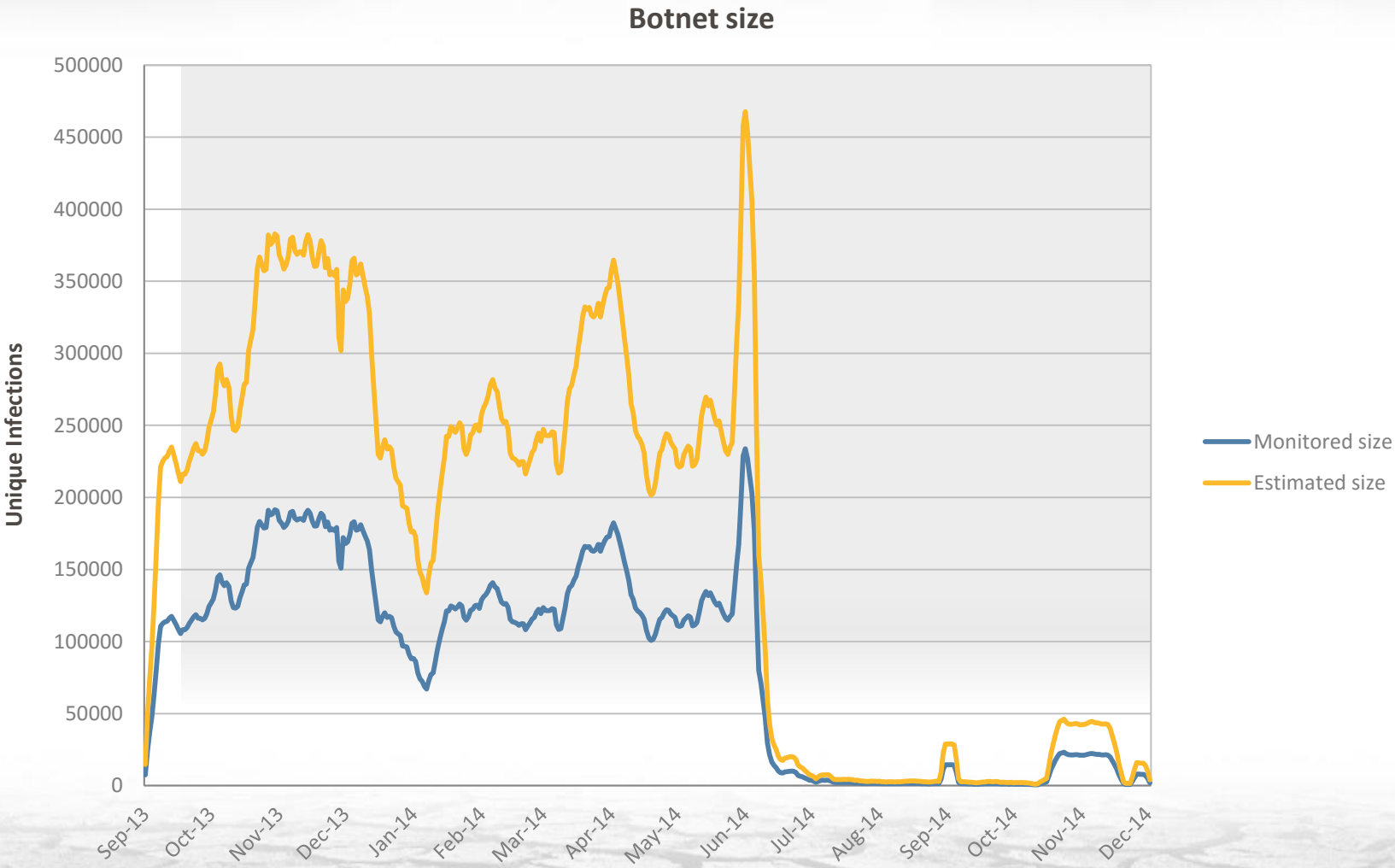
FBI PLANNED TAKEDOWN OPERATION JUNE 2014:

- Sinkhole the botnet
  - Redirect up to 1k domains to FBI owned infrastructure
  - New domains generated on 1st, 7th, 14th, 21st and 28th of each month
- Seize a number of supernodes
  - Supernodes communicate directly with C2

Private industry helps with remediation

- AV and IPS coverage
- Provide Fix Tool freely available to public
- Provide technical assistance/details (reverse engineer malware)
- Monitor and provide statistics of botnet size

Outcome


Botnet size
Unique Infections
500000
450000
400000
350000
300000
250000
200000
150000
100000
50000
0
Sep-13
Oct-13
Nov-13
Dec-13
Jan-14
Feb-14
Mar-14
Apr-14
May-14
Jun-14
Jul-14
Aug-14
Sep-14
Oct-14
Nov-14
Dec-14
Monitored size
Estimated size

LE involvement in takedowns

Gameover Zeus

FBI Leads Multi-National Action, seizing a global network of computer servers known as Gameover Zeus Botnet used by cyber-criminals to spread malware viruses and steal millions of dollars from businesses and consumers.

Gameover Zeus botnet:

- employing an estimated 500,000 to 1 million compromised computers
- more than $100 million in losses

INDUSTRY COOPERATION

SMEs: Dell SecureWorks, Crowdstrike, Shadowsever, Spamhaus, NCFTA

TOP LEVEL DOMAIN (TLD) REGISTRIES

Afilias

neustar

Your Public Interest Registry

VERISIGN

ISPs

ICANN

Operation Clean Slate

DHS/US-CERT

Anti-Virus Companies

Symantec

TREND MICRO

SOPHOS

F-Secure

HEIMDAL SECURITY

Microsoft

SYMANTEC PROPRIETARY/CONFIDENTIAL – INTERNAL USE ONLY
Copyright © 2012 Symantec Corporation. All rights reserved.