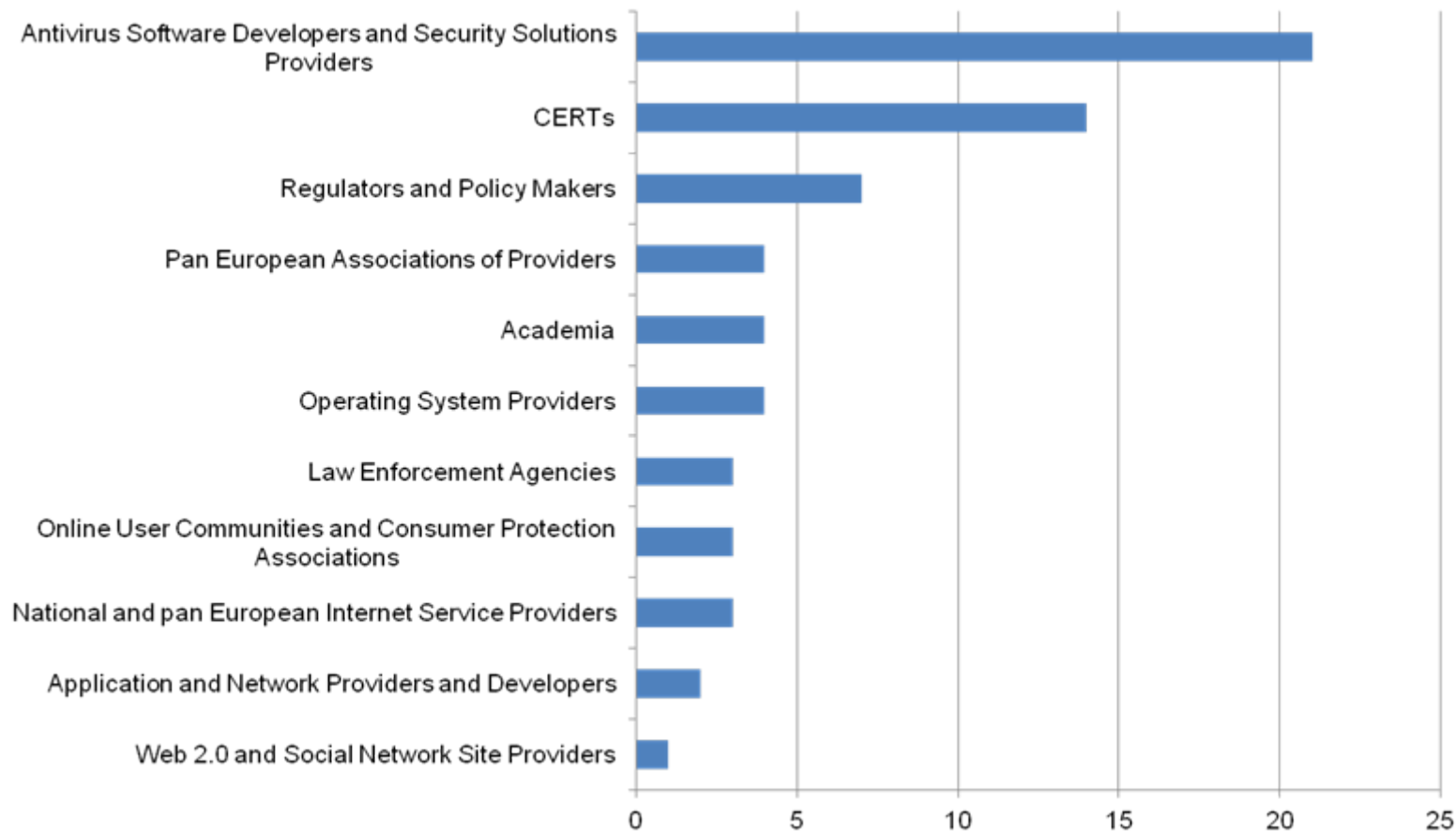


Botnets – Measurement and Defence

Dr Giles Hogben
Programme Manager for Secure Services
28 January 2010

Who we consulted



Overview

- ★ Measurement and detection
- ★ Countermeasures
 - Threat picture
 - Roles, responsibilities and incentives
- ★ Legal issues

The need to assess the threat level

- **Deciding on investments (100's of millions of Euros):** in security measures.
- **Defining the political agenda:** Botnets are a major threat to society.
- **Assessing the success of measures:** how do we know a technique worked

Measurement and Detection

★ Problems identified with current measures

- ★ Lack of accuracy
- ★ Transparency of methodology
- ★ Incentives for exaggeration



Size is not everything

Researchers Tracking Emerging 'Darkness' Botnet

Posted by [Soulskill](#) on Tuesday December 07, @01:35AM
from the new-kid-on-the-block dept.



Trailrunner7 writes

"Researchers are tracking a new botnet that [has become one of the more active DDoS networks on the Internet](#) since its emergence early last month. The botnet, dubbed 'Darkness,' is being [controlled by several domains hosted in Russia](#) and its operators are boasting that it can take down large sites with as few as 1,000 bots. The Darkness botnet is seen as something of a successor to the older Black Energy and Illusion botnets and researchers at the Shadowserver Foundation took a look at the network's operation and found that it is capable of generating large volumes of attack traffic. 'Upon testing, it was observed that the throughput of the attack traffic directed simultaneously at multiple sites was quite impressive,' Shadowserver's analysts wrote in a report on the Darkness botnet. 'It now appears that "Darkness" is overtaking Black Energy as the DDoS bot of choice. There are many ads and offers for DDoS services using "Darkness." It is regularly updated and improved and of this writing is up to version 7. There also appear to be no shortage of buyers looking to add "Darkness" to their botnet arsenal.'"

- From Panda Labs: order of 500 computers (not a botnet but some characteristics in common) took down Visa.com during the Anonymous attacks
- But nobody ever quotes anything else



COUNTERMEASURES AND RECOMMENDATIONS

Goal: Minimize botnet threat

Direction	Mitigate existing botnets		Prevent new infections		Minimize profitability of botnets		
Approach	Reduce number of infected systems	Fight C&C infrastructure	Slow down botnet spreading through early detection	Protect systems User awareness	Increase security awareness	Attack botnet value creation chain	
Preconditions	Reliable method for the detection of infections	Analysis of C&C infrastructures	Analysis of structures and patterns	Identification of vulnerabilities	Identification of primary assets of criminal value creation chain		
Auxiliaries	Host anti-MW software	Network ISPs	Information sharing, tracking of botnets	Identification of C&C and comm. patterns	Exploit discovery and information sharing	Information campaigns and security education	Derive botnet functionality and economics
Actions	Cleaning of systems	Takedown of C&C and arrest of botmasters	Application of preventive measures	Responsible operation, patching of systems	Active support of users	Improve anti-fraud, prosecute botmasters, create deterrence	

Mitigate Existing Botnets

Mitigate existing botnets

Reduce number of infected systems

Fight C&C infrastructure

Reliable method for the detection of infections

Analysis of C&C infrastructures

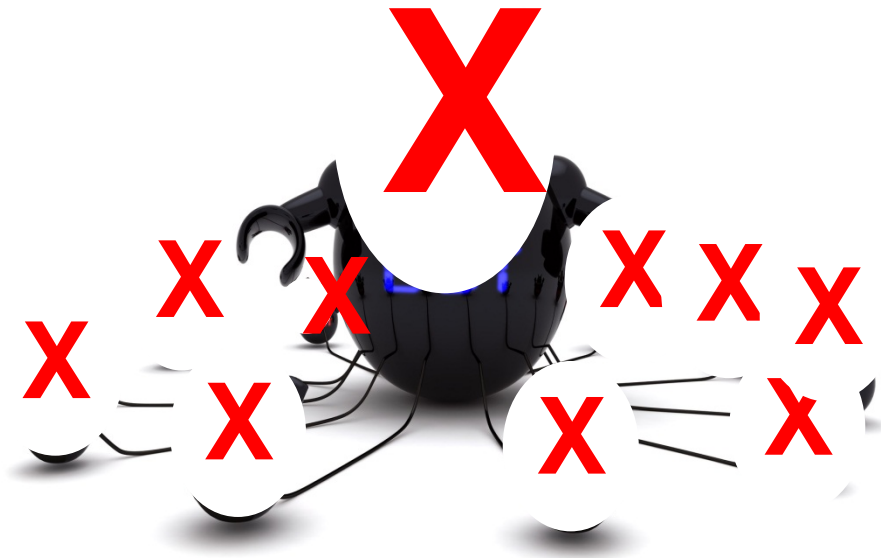
Host-level
anti-MW
software

Netw.-level
ISPs

Information
sharing, tracking of
botnets

Cleaning of
systems

Takedown of C&C
and arrest of
botmasters



Prevent new infections

Slow down botnet
spreading through
early detection

Protect systems
User awareness

Analysis of
structures and
patterns

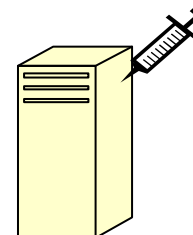
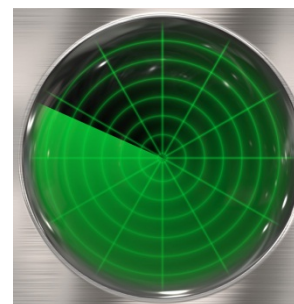
Identification of
vulnerabilities

Identification of
C&C and comm.
patterns

Exploit discovery
and information
sharing

Application of
preventive
measures

Responsible
operation, patching
of systems



Minimize profitability of botnets

Increase security awareness

Attack botnet value creation chain

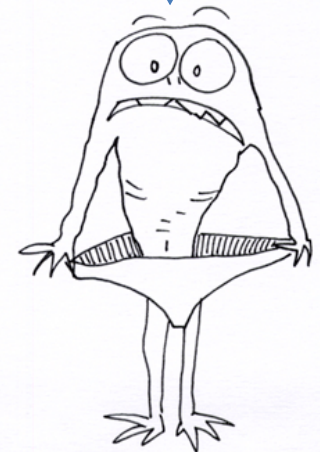
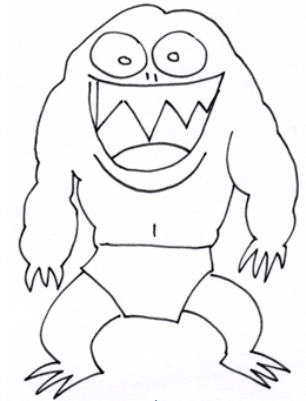
Identification of primary assets of criminal value creation chain

Information campaigns and security education

Derive botnet functionality and economics

Active support of users

Improve anti-fraud and prosecute botmasters



Botnet countermeasures

★ Technical

- Blacklisting
- Distribution of Fake & Traceable Credentials
- BGP Blackholing
- DNS-based methods
- Takedown of C&C Servers
- Packet Filtering / Port 25 Handling
- Walled Gardens
- P2P Countermeasures
- Remote Disinfection

★ Social and Policy

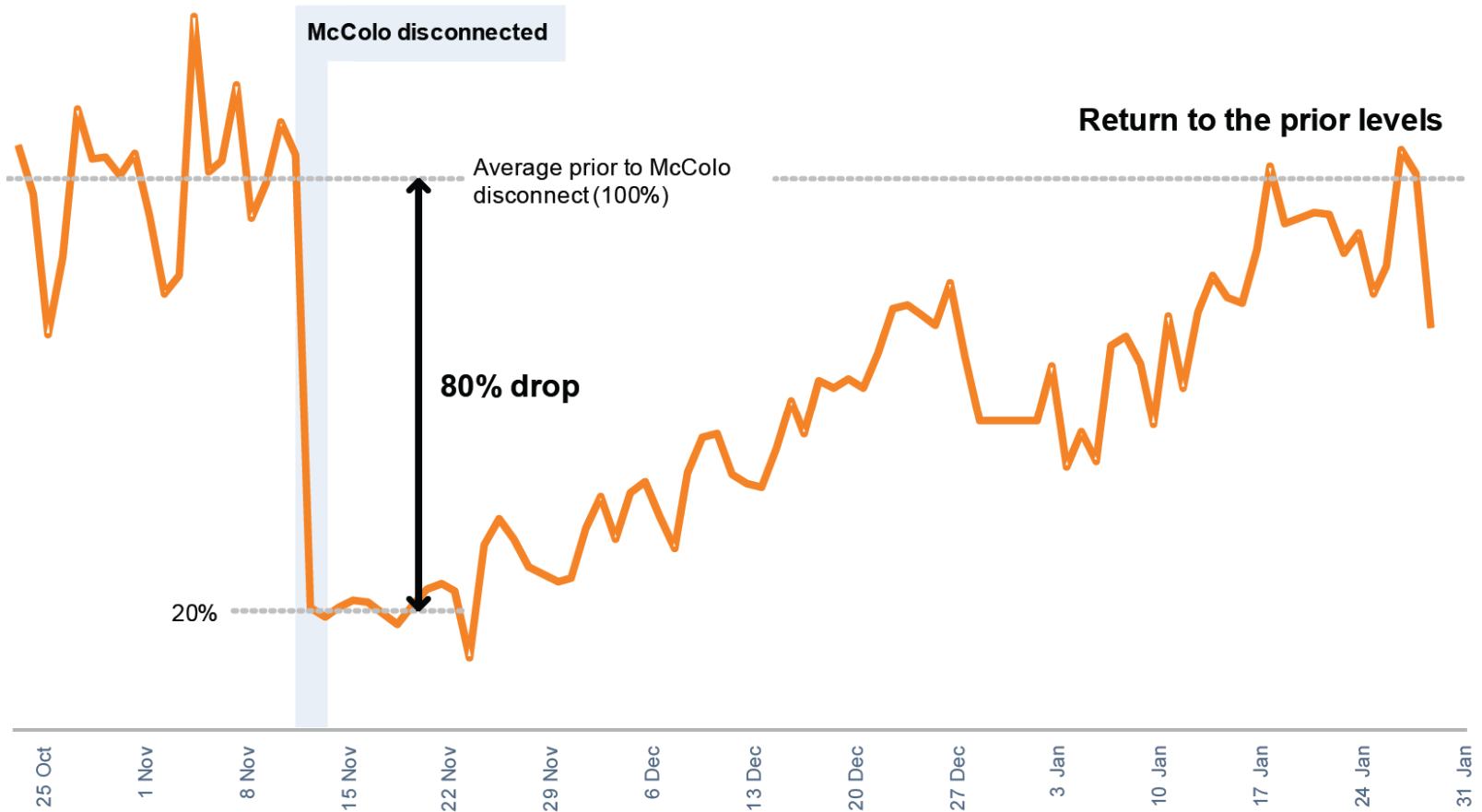
- Dedicated Laws on Cybercrime
- User Awareness raising and Special Training
- Central Incident Helpdesks
- Enhance Cooperation between Stakeholders

Example Key Challenge

Actions against botnet C&C infrastructure do not affect infections in the long-term

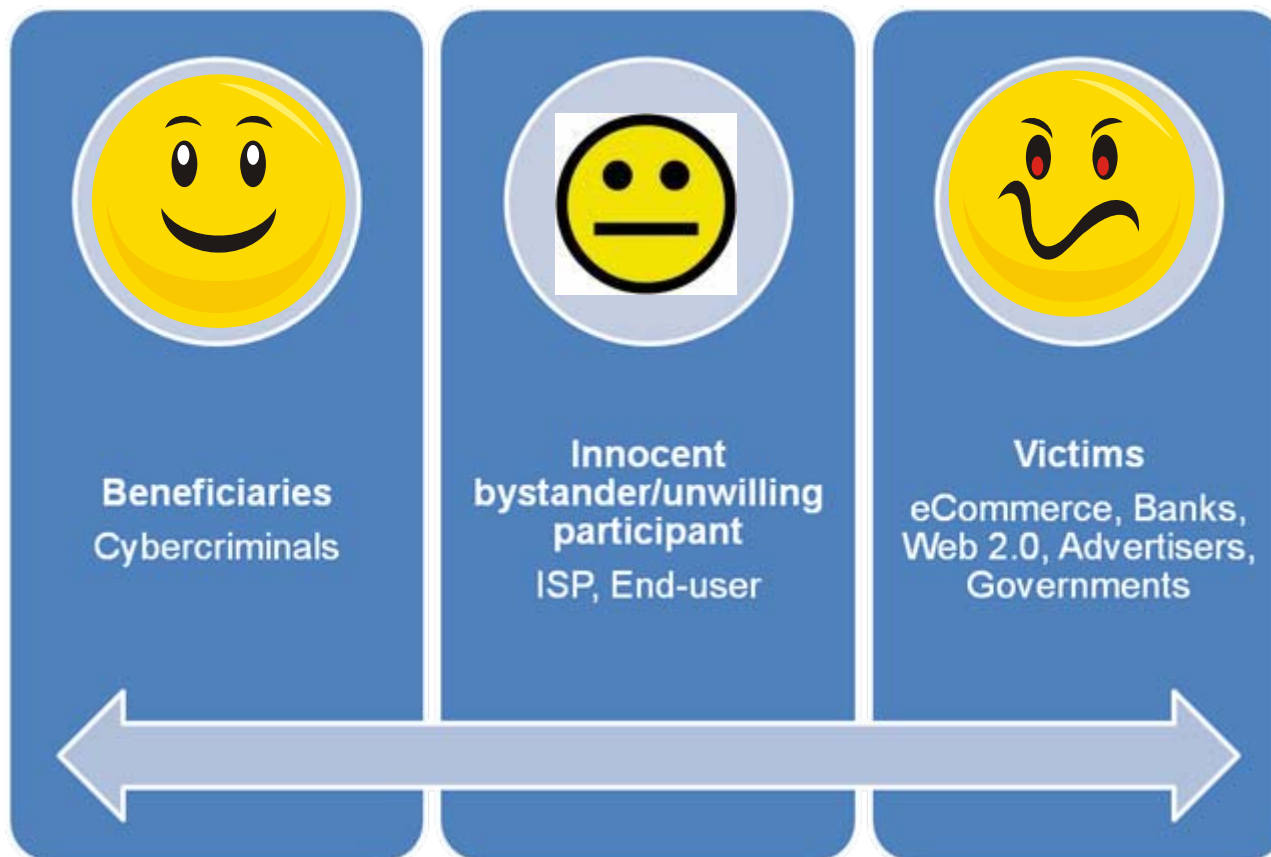
Incomplete takedowns may raise botnet resilience

- ★ Infrastructure may be migrated after regaining control
- ★ „Teaching“ botmasters to update and enhance

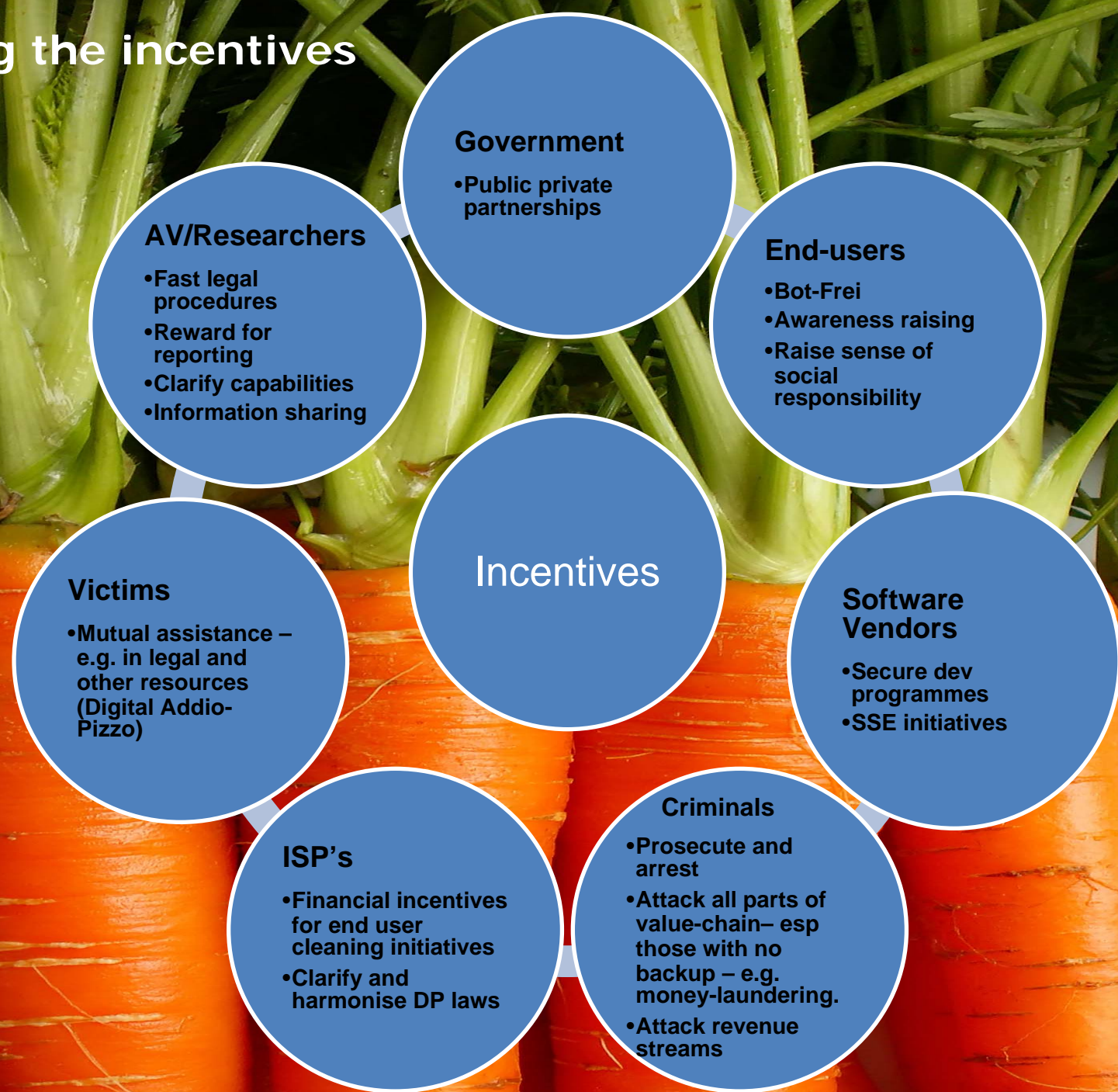




Current incentives



Rebalancing the incentives



ENISA reports

- Botnets: Detection, measurement, disinfection and defence – best practice and analysis.
<http://www.enisa.europa.eu/botnets>
- Botnets: 10 tough questions – Analysis by ENISA and expert group.
<http://www.enisa.europa.eu/botnets-10Q>
- Legal analysis and recommendations. In preparation