Botnets: Measurement, Detection, Disinfection and Defence

Dr Giles Hogben

ENISA

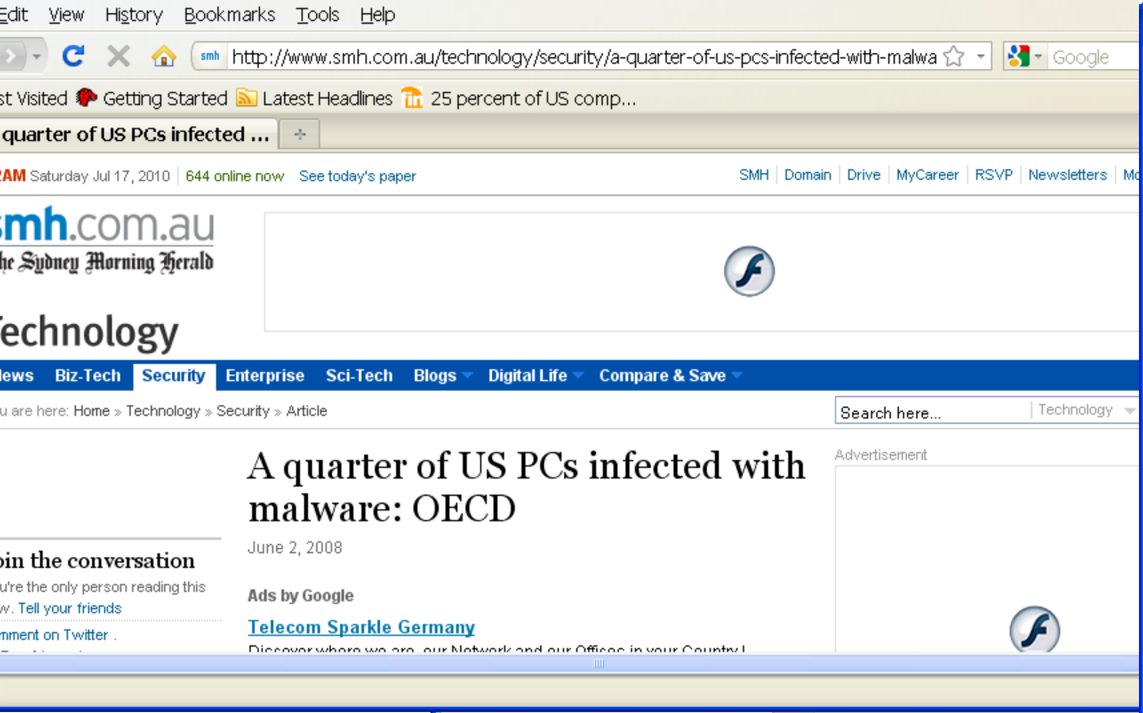
Overview

- Recommendations
  - Measurement and detection
  - Countermeasures
    - Threat picture
    - Roles, responsibilities and incentives
  - Focus on legal issues, information sharing

MEASUREMENT AND DETECTION

The need to assess the threat level

- **Deciding on investments (100’s of millions of Euros):** in security measures. For governments as well as for businesses.
- **Defining the political agenda:** Botnets are a major threat to society to be engaged on governmental level.
- **Assessing the success of measures:** how do we know a technique worked



Edit View History Bookmarks Tools Help
http://www.smh.com.au/technology/security/a-quarter-of-us-pcs-infected-with-malwa
Google
st Visited Getting Started Latest Headlines 25 percent of US comp...
quarter of US PCs infected ...
AM Saturday Jul 17, 2010 644 online now See today's paper
SMH Domain Drive MyCareer RSVP Newsletters
smh.com.au
he Sydney Morning Herald
echnology
ews Biz-Tech Security Enterprise Sci-Tech Blogs Digital Life Compare & Save
u are here: Home » Technology » Security » Article
Search here...
Technology
Advertisement

A quarter of US PCs infected with malware: OECD

June 2, 2008

oin the conversation

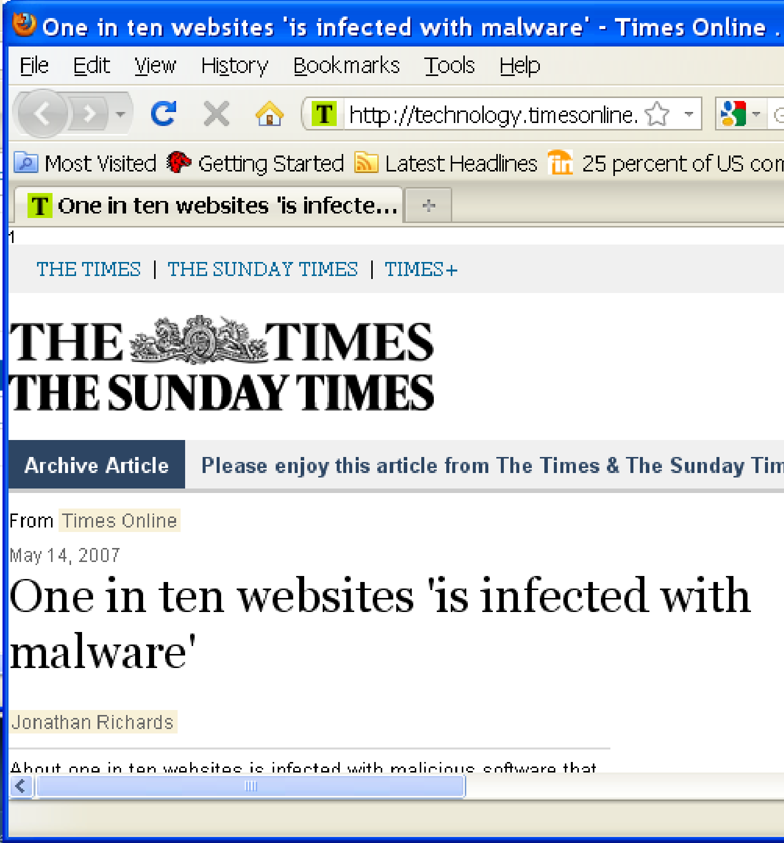
u're the only person reading this w. Tell your friends

mment on Twitter .

Ads by Google

Telecom Sparkle Germany

Discover where we are, our Network and our Offices in your Country!



One in ten websites 'is infected with malware' - Times Online
File Edit View History Bookmarks Tools Help
http://technology.timesonline.
Most Visited Getting Started Latest Headlines 25 percent of US com
One in ten websites 'is infecte...
THE TIMES | THE SUNDAY TIMES | TIMES+
THE TIMES
THE SUNDAY TIMES
Archive Article
Please enjoy this article from The Times & The Sunday Tim

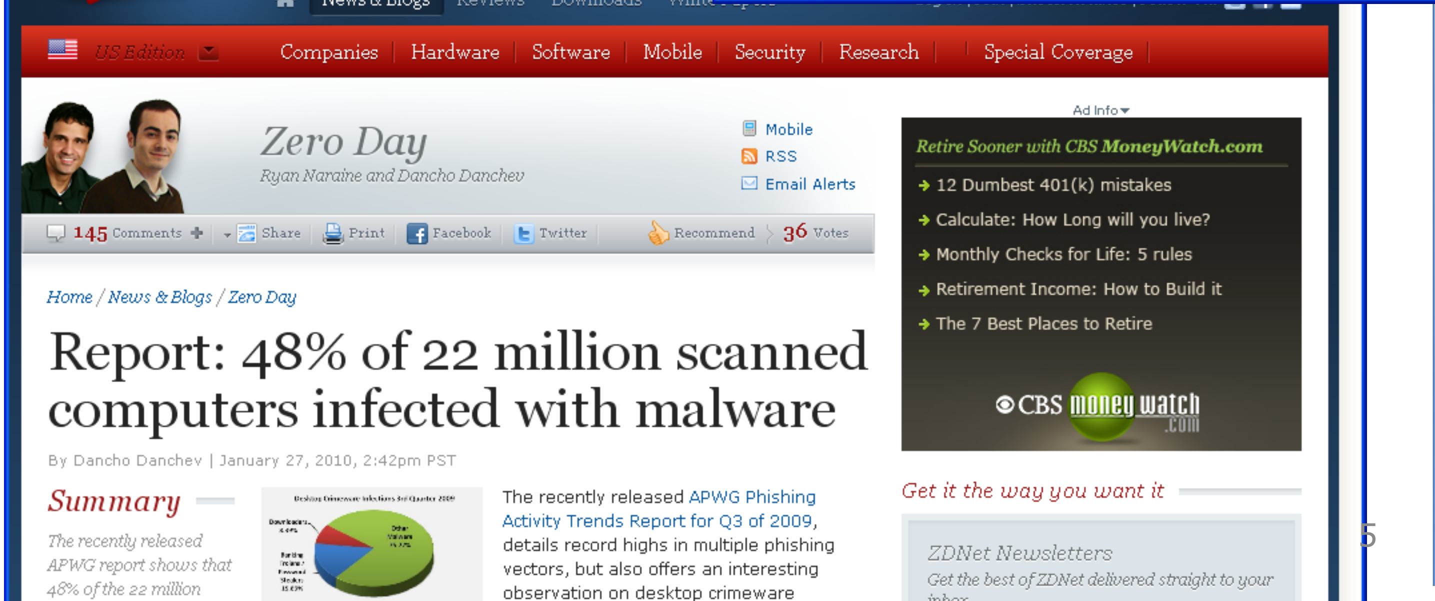
From Times Online

May 14, 2007

One in ten websites 'is infected with malware'

Jonathan Richards

About one in ten websites is infected with malicious software that



ZDNet
News & Blogs Reviews Downloads White Papers
US Edition
Companies Hardware Software Mobile Security Research Special Coverage
Zero Day
Ryan Naraine and Dancho Danchev
Mobile
RSS
Email Alerts
145 Comments
Share
Print
Facebook
Twitter
Recommend
36 Votes
Ad Info
Retire Sooner with CBS MoneyWatch.com
12 Dumbest 401(k) mistakes
Calculate: How Long will you live?
Monthly Checks for Life: 5 rules
Retirement Income: How to Build it
The 7 Best Places to Retire
CBS moneywatch.com
Get it the way you want it
ZDNet Newsletters
Get the best of ZDNet delivered straight to your inbox

Home / News & Blogs / Zero Day

Report: 48% of 22 million scanned computers infected with malware

By Dancho Danchev | January 27, 2010, 2:42pm PST

Summary

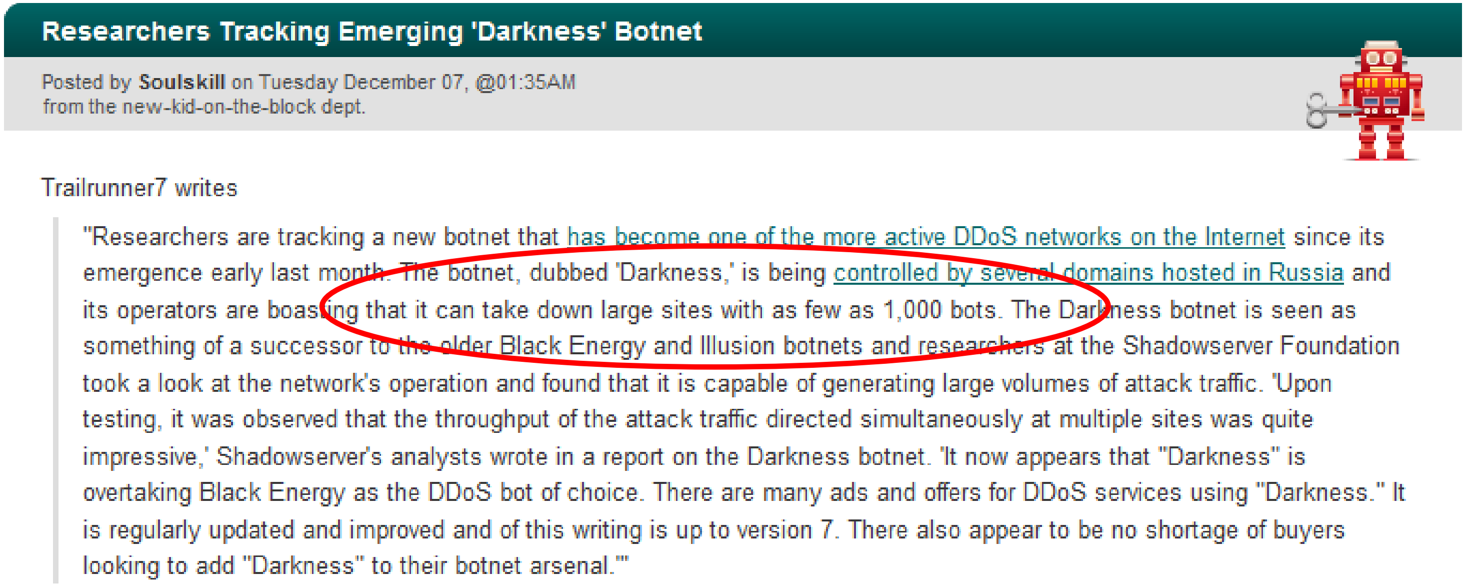
The recently released APWG report shows that 48% of the 22 million

The recently released APWG Phishing Activity Trends Report for Q3 of 2009, details record highs in multiple phishing vectors, but also offers an interesting observation on desktop crimeware

Measurement and Detection

- Problems identified with current measures
  - Lack of accuracy
  - Transparency of methodology
  - Incentives for exaggeration
  - Size is not everything

Size is not everything



Researchers Tracking Emerging 'Darkness' Botnet

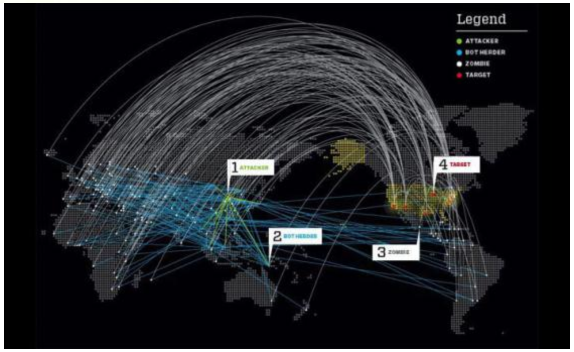
Posted by **Soulskill** on Tuesday December 07, @01:35AM
from the new-kid-on-the-block dept.

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

Impact depends on stakeholders



- Governments care about targeted theft of classified information and political/military targets.
- Financial organisations care about financial fraud and DDoS
- Email services care about spam volume.
- E-commerce providers care about DDoS attacks.

Better impact indicators

- Distribution (origin)
- Spam statistics
- Bandwidth of attacks
- Data types harvested
- Financial damage
- Malware characteristics

KEY RECOMMENDATIONS FOR COUNTERMEASURES

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

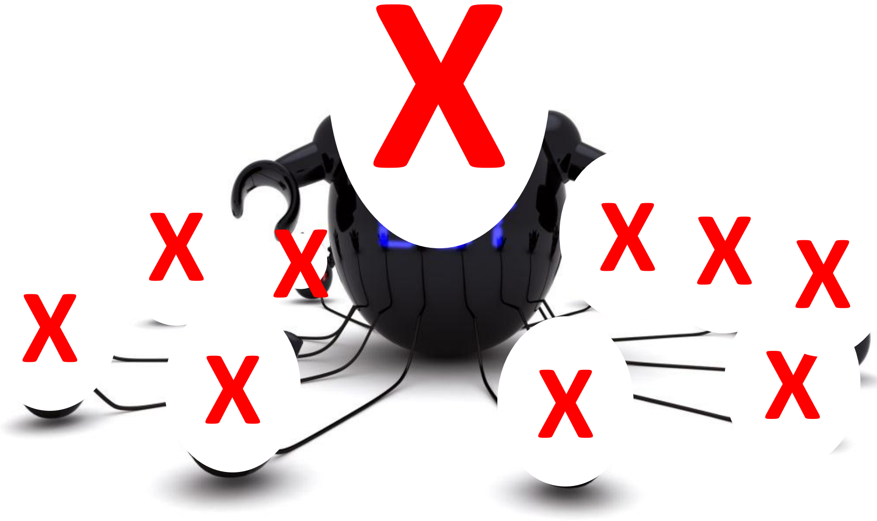
Host-level anti-MW software

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

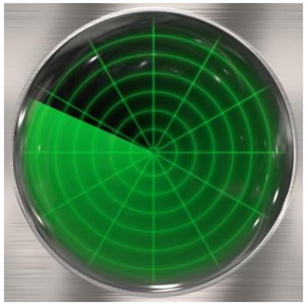
Identification of vulnerabilities

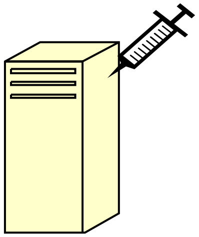
Identification of C&C and comm. patterns

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

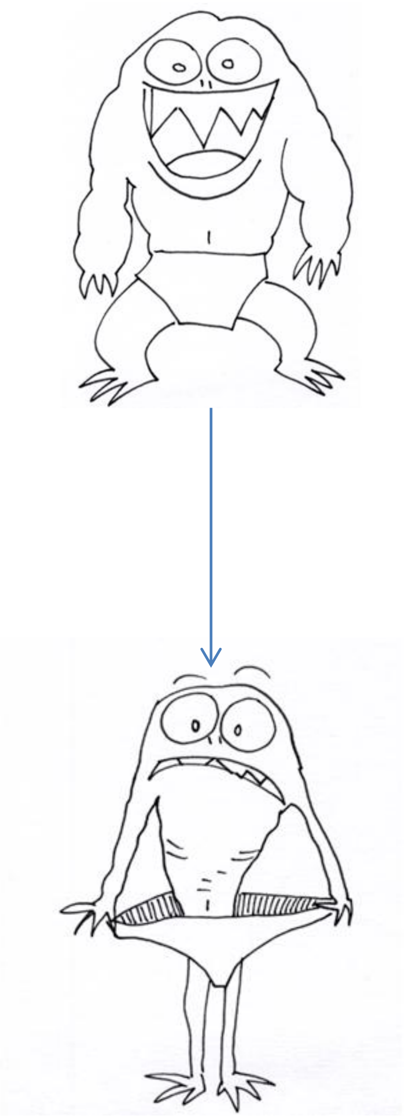
Identification of primary assets of criminal value creation chain

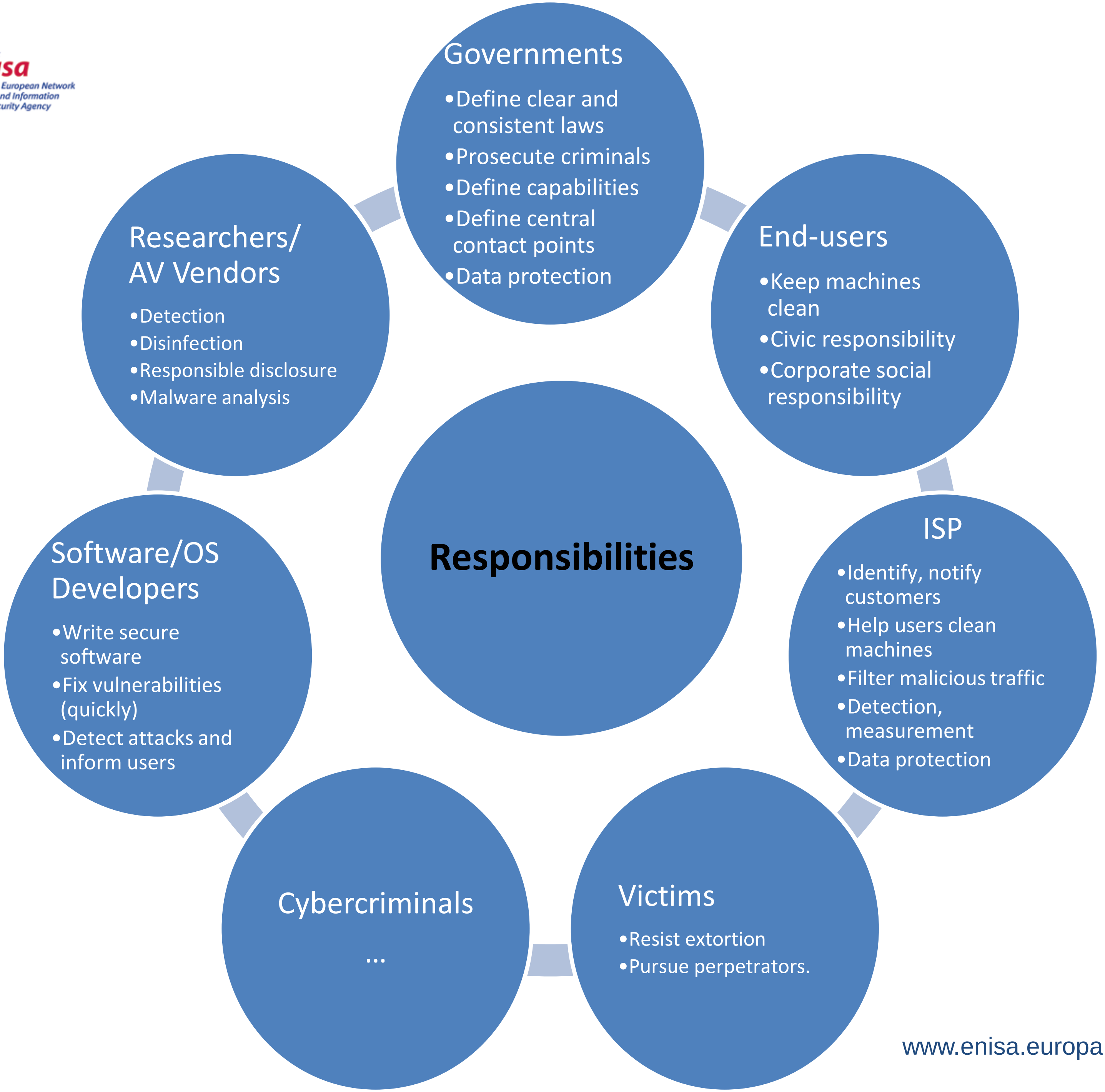
Information campaigns and security education

Derive botnet functionality and economics

Active support of users

Improve anti-fraud and prosecute botmasters





Responsibilities

Governments

- Define clear and consistent laws
- Prosecute criminals
- Define capabilities
- Define central contact points
- Data protection

End-users

- Keep machines clean
- Civic responsibility
- Corporate social responsibility

ISP

- Identify, notify customers
- Help users clean machines
- Filter malicious traffic
- Detection, measurement
- Data protection

Victims

- Resist extortion
- Pursue perpetrators.

Cybercriminals

…

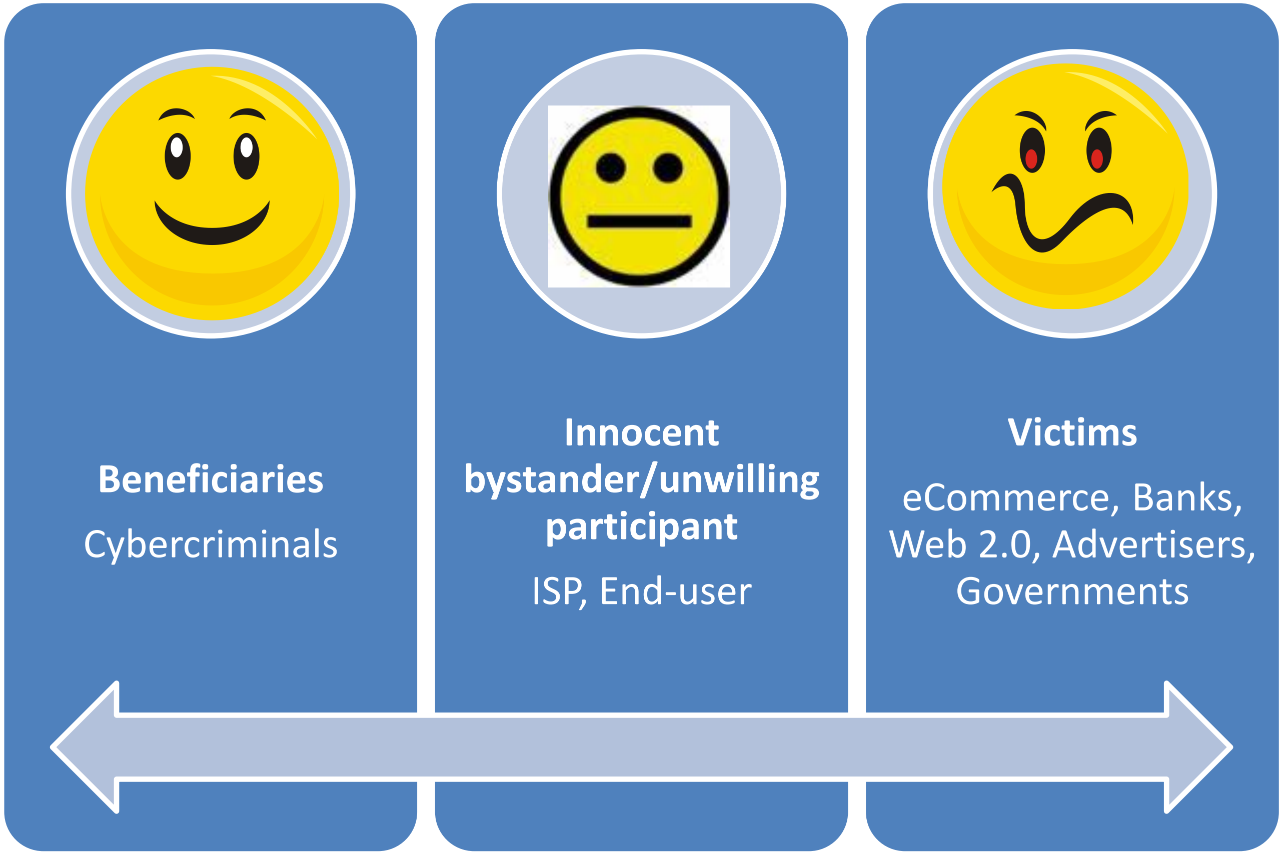
Software/OS Developers

- Write secure software
- Fix vulnerabilities (quickly)
- Detect attacks and inform users

Researchers/ AV Vendors

- Detection
- Disinfection
- Responsible disclosure
- Malware analysis

Current incentives



Beneficiaries

Cybercriminals

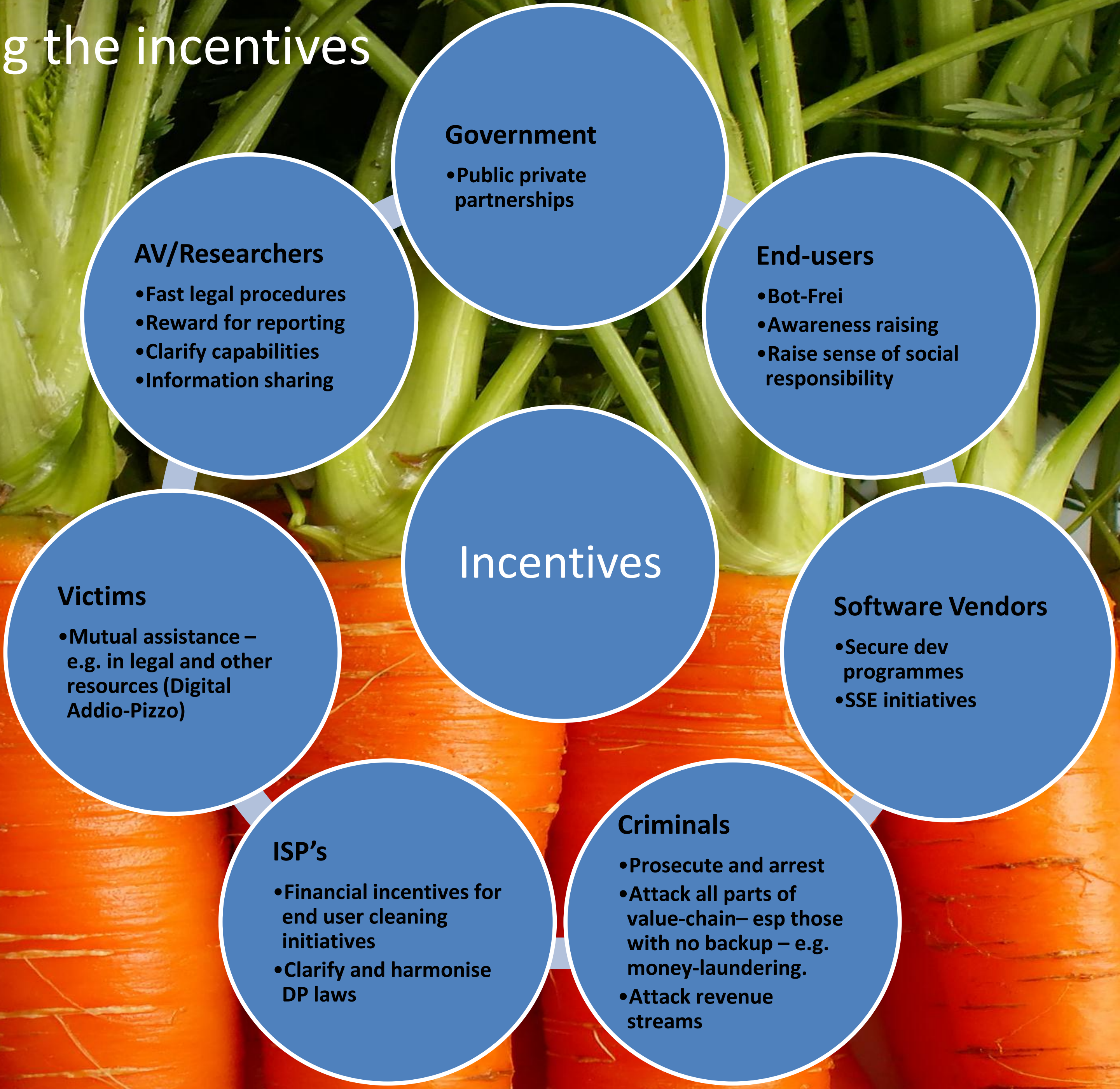
Innocent bystander/unwilling participant

ISP, End-user

Victims

eCommerce, Banks, Web 2.0, Advertisers, Governments

Rebalancing the incentives



Incentives

Government

- Public private partnerships

End-users

- Bot-Frei
- Awareness raising
- Raise sense of social responsibility

Software Vendors

- Secure dev programmes
- SSE initiatives

Criminals

- Prosecute and arrest
- Attack all parts of value-chain– esp those with no backup – e.g. money-laundering.
- Attack revenue streams

ISP’s

- Financial incentives for end user cleaning initiatives
- Clarify and harmonise DP laws

Victims

- Mutual assistance – e.g. in legal and other resources (Digital Addio-Pizzo)

AV/Researchers

- Fast legal procedures
- Reward for reporting
- Clarify capabilities
- Information sharing

Information sharing

- Benefits
  - Coordination
  - View on trends
  - Faster reaction
- Challenges
  - Abuse report formats
  - Mutually beneficial sharing
  - Trust between parties.
  - Confidentiality - how to know when 2 teams are infiltrating the same botnet without alerting the botmaster?

Legal and Jurisdictional challenges

- Clear definition of who can do what in the EU 27 and beyond.
  - E.g. Status of IP address as Private Data
- Roles and responsibilities – points of contact across border – vide ENISA exercise.
- Empower people who are in a position to do something and clarify what
  - e.g. define clearly what botbusters can and cannot do.
  - E.g. Good samaritan provisions.
  - Quick reaction by law enforcement and justice.
  - Accelerated procedures – time is premium
- Find practical balance between DP laws and system security.

Legal Report

- Work in progress: separate report on legal issues Q2 based on survey of experts at EU and MS level.
- Stakeholder capabilities e.g. Packet inspection, Takedown, Remote disinfection
- Emergency powers
- Liability of stakeholders (for damages, non-action, disclosure)
- Gaps and recommendations

Key messages

- We don’t have good enough information on threat levels.
- Provide the right incentives to those in a position to fight botnets.
- Efficient and comprehensive international co-operation
- Clarify and harmonise legislation

Questions?

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

Group Composition

- National and pan European Internet Service Providers: 3
- Antivirus Software Developers and Security Solutions Providers: 21
- Operating System Providers: 4
- Application and Network Providers and Developers: 2
- Web 2.0 and Social Network Site Providers: 1
- Academia: 4
- CERTs: 14
- Online User Communities and Consumer Protection Associations: 3
- Regulators and Policy Makers: 7
- Law Enforcement Agencies: 3
- Pan European Associations of Providers: 4