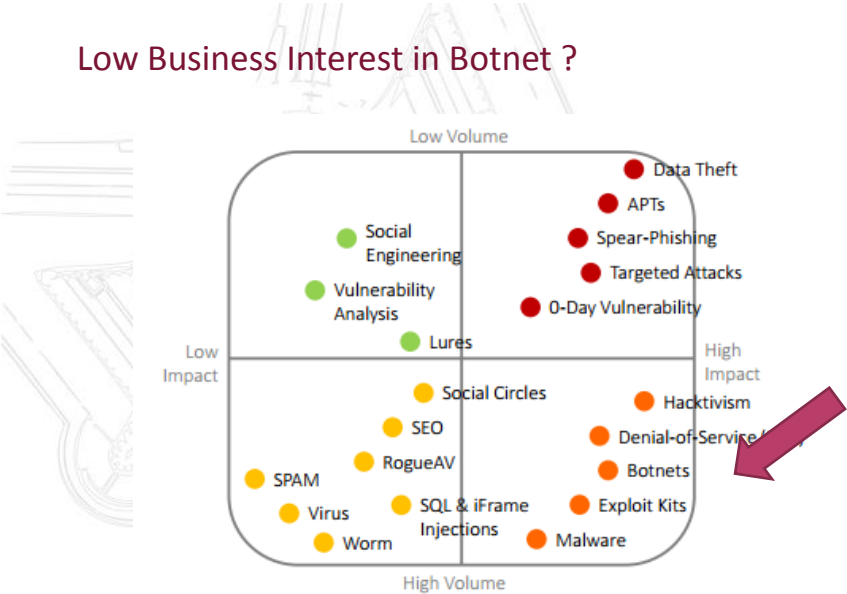


Advanced Cyber Defence Center

Botconf 2013

Nantes, Dec 5th 2013

Ulrich Seldeslachts (MD | LSEC)  
ulrich@lsec.be | +32 16 32 8541





ACDC  
&  
The European Commission's  
Cyber Security Strategy

Trust and Security  
DG CONNECT - European Commission



## ACDC Cybersecurity the need for further EU action



1. Economic and social benefits of the Digital Single Market
2. Risks and incidents on the rise > Lack of trust, economic losses, missed opportunities
3. Cross-border nature of risks and incidents
4. Insufficient national preparedness and cooperation across the EU

***EU Cybersecurity Strategy Objective and Priorities : "To ensure a safe and resilient digital environment in respect of fundamental rights and EU core values"***

1. Legislative proposal on Network and Information Security (NIS)
2. Fighting botnets, ensuring the security and resilience of Industrial Control Systems and Smart grids
3. Awareness raising
4. Public-Private Partnerships

© Leaders in Security – LSEC, 2013, Private & Confidential, p 5



## ACDC Significance of ACDC for the EC Strategy



- **First Element of the Strategy to be launched**
- **First test to prove Commissioner Kroes points:**
  - "[cybersecurity] can only happen when all actors play their part and take up their responsibilities."
  - "Cyber threats are not contained to national borders: nor should cybersecurity be"
- **Conclusion: success of ACDC central to success European cybersecurity policies**

© Leaders in Security – LSEC, 2013, for ACDC – public, p 6





## Facts and Figures



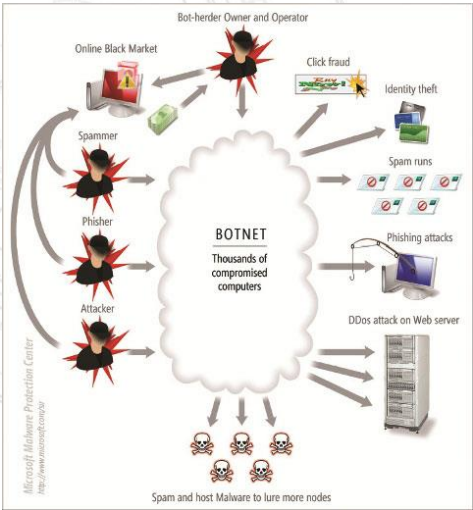
- **EC CIP PSP Project :** (CIP-ICT PSP-2012-6 - Obj. 5.1: Cyber security Pilot B)
  - 2012 European Commission Competitiveness and Innovation Program
  - Policy Support Program
  - Pilot Action B : pilot action against botnets
- **Consortium:** 28 partners from 14 Member States
- **Budget:** 15.5 mio € - 50% support by the EC
- **Duration :** 01. FEB 2013 until FEB 2016

© Leaders in Security – LSEC, 2013, for ACDC – public , p 7

7



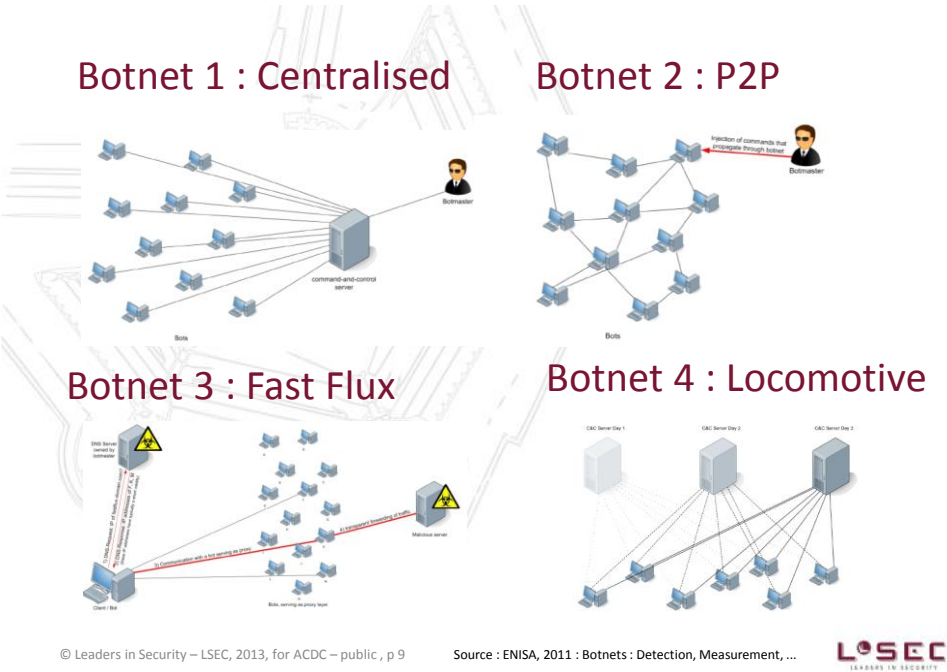
## What you know : how a botnet works




© Leaders in Security – LSEC, 2013, for ACDC – public , p 8


Source : PCWorld








What you’ve found out : too many parties



	Objective 1 Tracking down C&C, com. channels, botnet masters	Objective 2 Removing bots from infected computers	Objective 3 Removing malware from web sites and services	Objective 4 Mitigating the impact of botnets
Law enforcement agencies	*		*	
Data Protection Agencies	*	*	*	
Government regulatory authorities	*	*	*	*
Government cybersecurity experts (e.g. CERTs)	*	*	*	*
ISPs	*	*	*	*
Financial institutions		*		
Managed security service providers	*		*	*
Web service/cloud providers	*	*		*
Web hosting providers	*		*	
Antivirus/Firewall/Scanner Vendors	*	*	*	*
Domain Name Service providers	*		*	
Domain Name Registrars	*		*	
Media		*		
Awareness raising initiatives		*		
Researchers	*	*	*	*
Software & Hardware producers	*	*		*

Source : ENISA, 2012 : DG INFSO CIP PSP

© Leaders in Security – LSEC, 2013, for ACDC – public , p 10


10 

 **28 partners – 14 member countries**



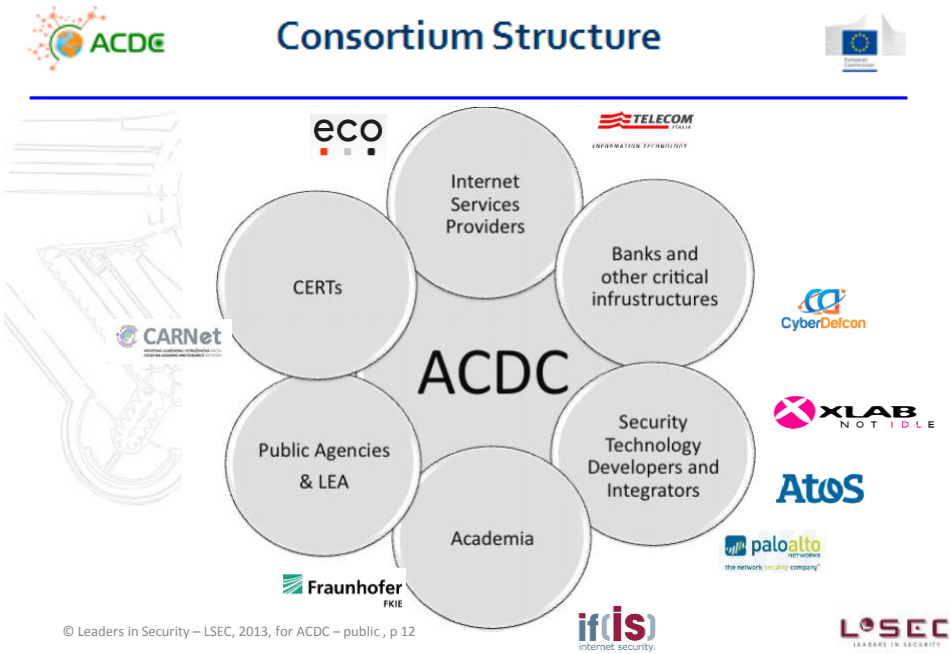
ECO Association of the German Internet Industry
Technikon Forschungs- und Planungsgesellschaft mbH
Atos Spain S.A
Bulgarian Posts PLC
Croatian Academic and Research Network - CARNet and Croatian National CERT
Romanian National Computer Emergency Response Team - CERT-RO & Romanian Partners
Cognitive Security s.r.o.
Cassidian (EADS Company)
CyberDefcon
DE-CIX
DFN CERT Services GmbH
Engineering Ingegneria Informatica
FCFN - Foundation for National Scientific Computing


ACDC Team




Fraunhofer FKIE
G Data Software AG
Institute for Internet Security, Gelsenkirchen University of Applied Sciences
INTECO - National Institute of Communication Technologies
KU Leuven
LSEC - Leaders in Security
Microsoft EMEA
SignalSpam
Telecom Italia
Telefonica I+D
University of Technology - Delft
XLAB Razvoj programske opreme in svetovanje d.o.o.
Fundació Privada Barcelona Digital Centre Tecnològic
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione
Montimage


© Leaders in Security – LSEC, 2013, for ACDC – public, p 11









































# EC Botnet Fighting Team












© Leaders in Security – LSEC, 2013, for ACDC – public , p 13

Source : ACDC Kickoff Meeting, DE-CIX, Frankfurt, 2013



LEADERS IN SECURITY

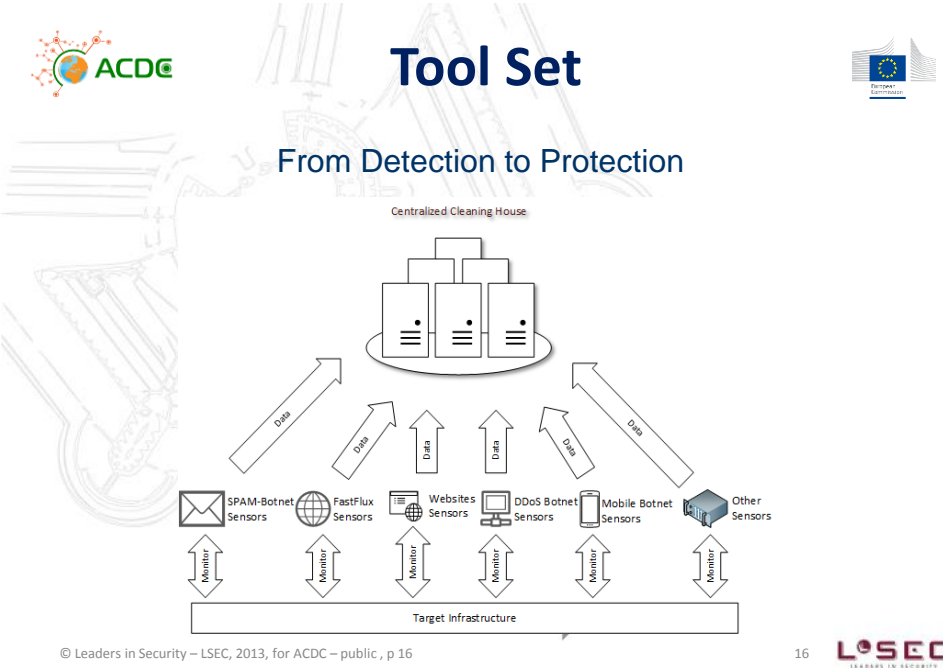


# Pan-European Approach



- ›extensive **sharing of information** – without borders:
  - across networks & member states
- ›provide a complete set of **solutions**:
  - accessible online for mitigating on-going attacks
- ›use the **pool of knowledge**
  - to create best practices
  - to support affected end customers & organisations in raising their cyber-protection level
- ›create a European wide network of cyber-defence centres

© Leaders in Security – LSEC, 2013, for ACDC – public , p 14

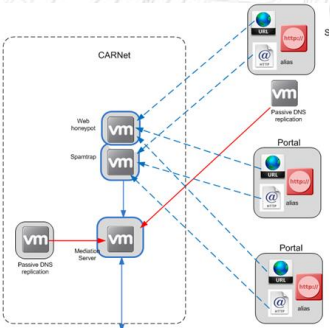




# Operational Detection



CARNet (KR) have produced a network of detection systems which Identify botnet activity within spam e-mails and network connections.



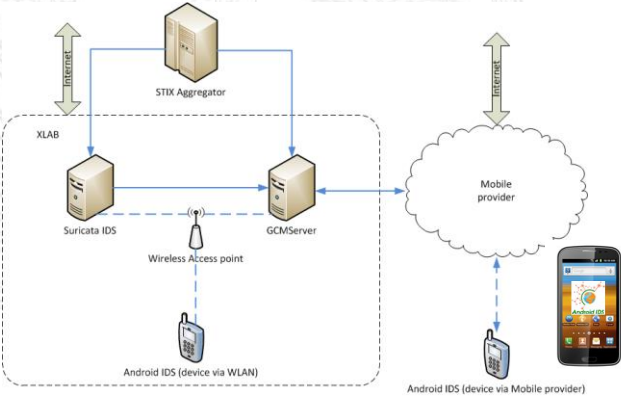
© Leaders in Security – LSEC, 2013, for ACDC – public , p 17



# Operational Detection



XLAB have produced an Intrusion Detection System for Android smart phones.



© Leaders in Security – LSEC, 2013, for ACDC – public , p 18

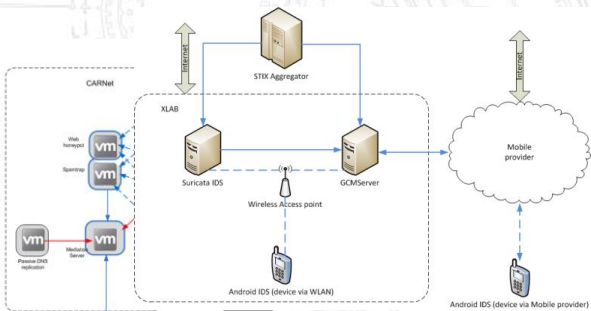




# Data Sharing & Analysis



CARNet creates identified threat information in the STIX format and sends the information to the ACDC STIX Aggregator



STIX Aggregator

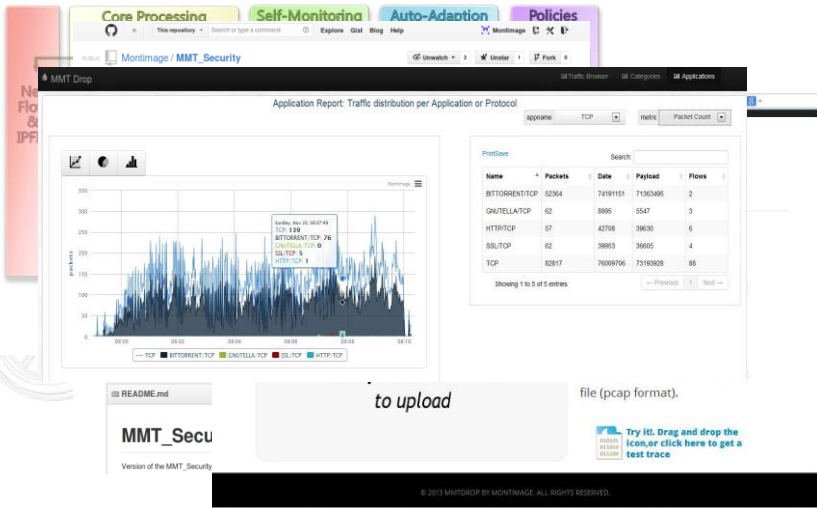


The XLAB Android IDS infrastructure queries the STIX Aggregator to obtain threat information provided by CARNet and blocks access to suspicious sites.


© Leaders in Security – LSEC, 2013, for ACDC – public, p 19



# Data Analysis




© Leaders in Security – LSEC, 2013, for ACDC – public, p 20





### Types of Information Currently Collected

- URLs hosting suspected malware
- Malware samples
- IP Addresses of hosts sending SPAM
- IP Addresses of suspected Command and Control Servers
- ...


Collected from Honeypot Networks, SPAM collection systems and Custom partner tools.

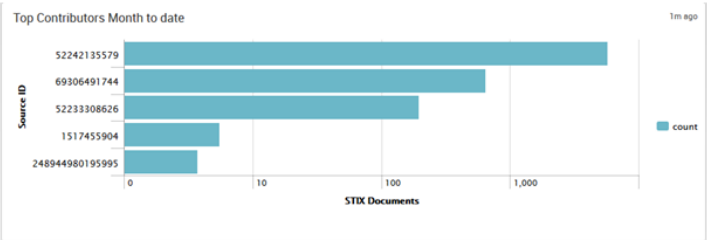







### Types of Information Currently Collected



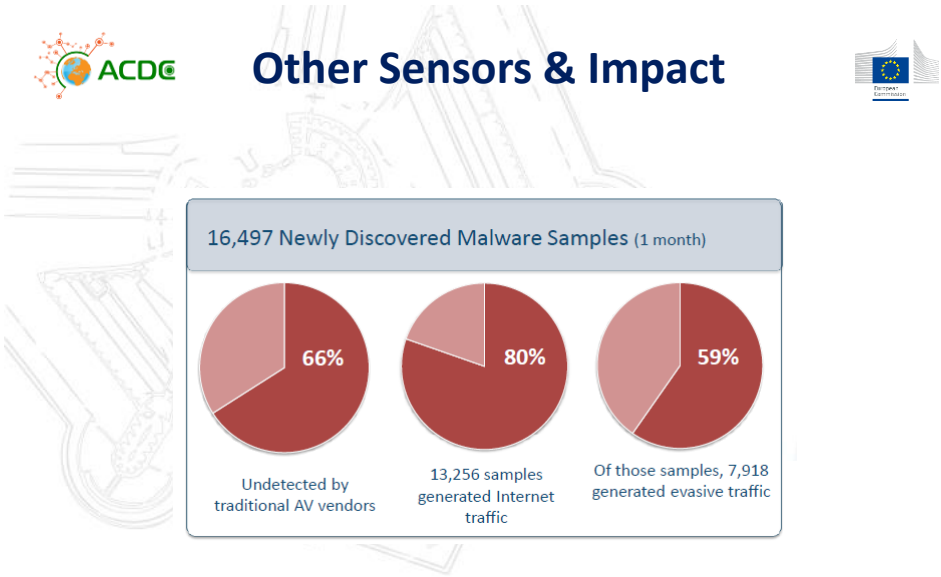
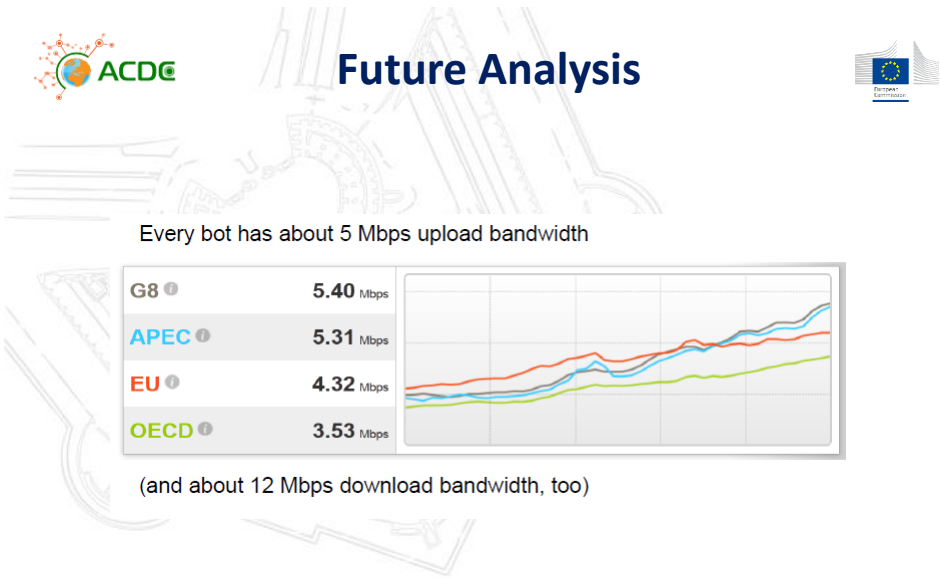




#### STIX Document Types Month to date




Indicators - Watchlist

Observations - Email






## User Tools & impact



<http://www.check-and-secure.com>

© Leaders in Security – LSEC, 2013, for ACDC – public, p 25

<https://www.check-and-secure.com/completion/ de/index.html>





## User Tools & Impact




<https://www.initiative-s.de/de/index.html>


© Leaders in Security – LSEC, 2013, for ACDC – public, p 26


<https://www.initiative-s.de/de/index.html>





# Sharing Impact







6f4a8be3f316 | 19114:UZ:21.493909 | CARNet Honeypot


© Leaders in Security – LSEC, 2013, for ACDC – public, p 27

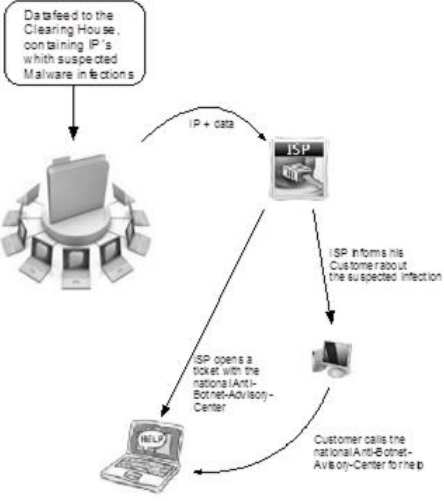
<http://stix.mitre.org/>






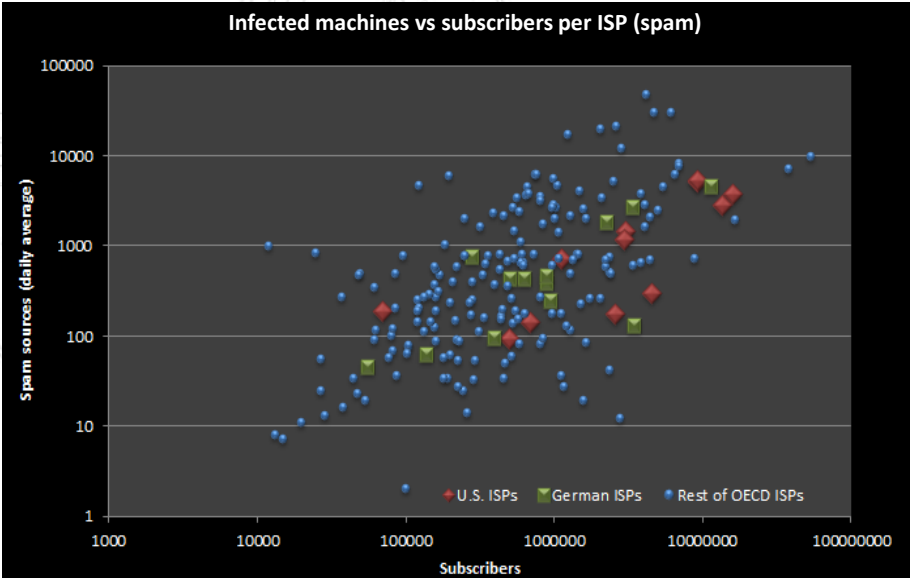
# Organization & User Impact





© Leaders in Security – LSEC, 2013, for ACDC – public, p 28

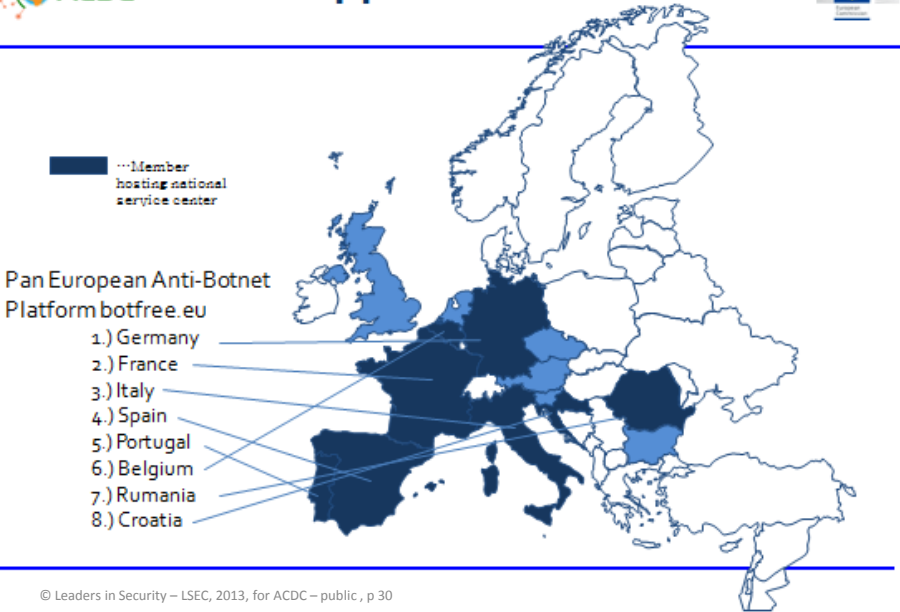





© Leaders in Security – LSEC, 2013, for ACDC – public , p 29      Source : Botnet mitigation and the role of ISPs, TU Delft, March 2013




## Support Centers



© Leaders in Security – LSEC, 2013, for ACDC – public , p 30





















## But, we need your help!










**Why is this one more dangerous than that one?**


- Size
- Infection Vector (Zero Day, downloaded by other, etc.)
- Monetization
- Damage
- Spreading
- ...

Pos. ?	Botnet
1	ZeroAccess
2	Conficker
3	Dorkbot
4	Salinity
5	Ramnit
6	Zeus





© Leaders in Security – LSEC, 2013, for ACDC – public , p 31

31 



## Join ACDC






Building Community Portal, Reaching out to :

industry, research, existing communities, law enforcement  
policy makers, isp's & operators, CERTs, ...

Looking for :

1. Detection & Mitigation Tools & Techniques
2. Data Analysis and Botnet Analysis & Prevalence
3. Data & Intelligence Sharing
4. Awareness Creation
5. Influencing Policy





© Leaders in Security – LSEC, 2013, for ACDC – public , p 32

32 

## NOT THE END

More information and follow-up

[www.acdc-project.eu](http://www.acdc-project.eu)

[www.botfree.eu](http://www.botfree.eu)



Q or C  
Ulrich Seldeslachts  
[ulrich@lsec.be](mailto:ulrich@lsec.be)  
+32 475 71 3602



© Leaders in Security – LSEC, 2013, Private & Confidential, p 33



## Links to Policy Documents



- Council conclusions on Critical Information Infrastructure Protection  
<http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf>
- Commission Communication on Critical Information Infrastructure Protection – "Achievements and next steps: towards global cyber-security" - COM(2011) 163  
[http://ec.europa.eu/information\\_society/policy/nis/docs/comm\\_2011/comm\\_163\\_en.pdf](http://ec.europa.eu/information_society/policy/nis/docs/comm_2011/comm_163_en.pdf)
- Digital Agenda for Europe - COM(2010)245 of 19 May 2010  
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF>
- The EU Internal Security Strategy in Action: Five steps towards a more secure Europe COM(2010)673  
[http://ec.europa.eu/commission\\_2010-2014/malmstrom/archive/internal\\_security\\_strategy\\_in\\_action\\_en.pdf](http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf)
- Commission Communication on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" - COM(2009) 149  
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF>

© Leaders in Security – LSEC, 2013, for ACDC – public, p 34

