Advanced Cyber Defense Center ACDC

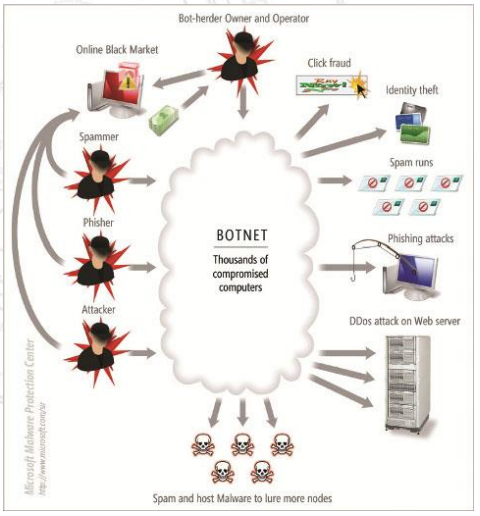
European Anti Botnet Pilot Action

Annual GI/ACM & EU Club R2Gs - ETSI ISG ISI

May 14, 2014

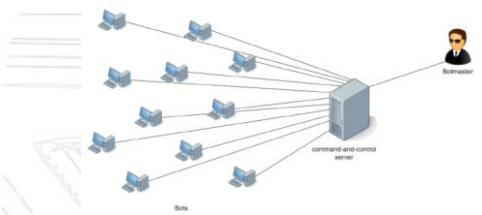
Ulrich Seldeslachts (MD | LSEC)
ulrich@lsec.be | +32 16 32 8541

What Botnets do

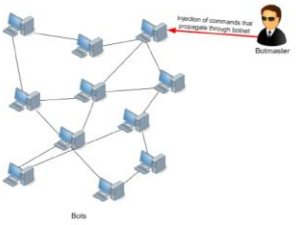


Source : PCWorld

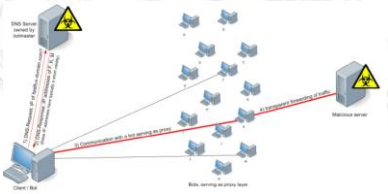
Botnet 1 : Centralised



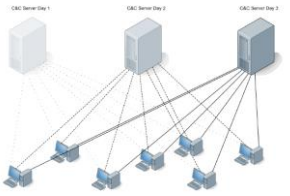
Botnet 2 : P2P



Botnet 3 : Fast Flux

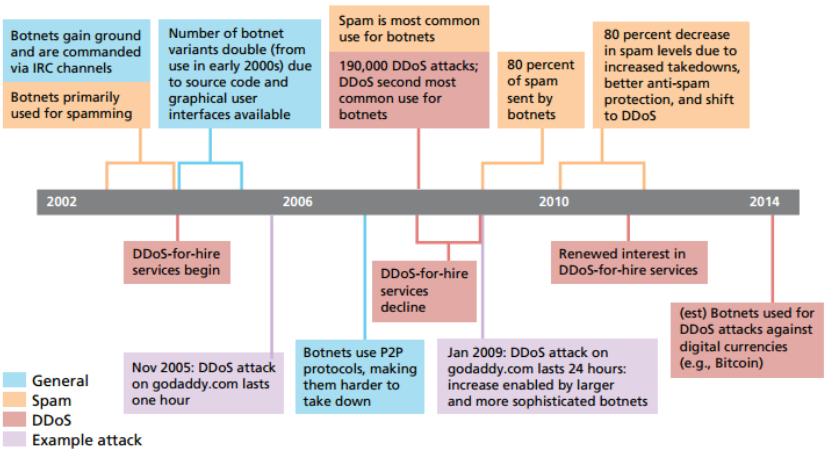


Botnet 4 : Locomotive



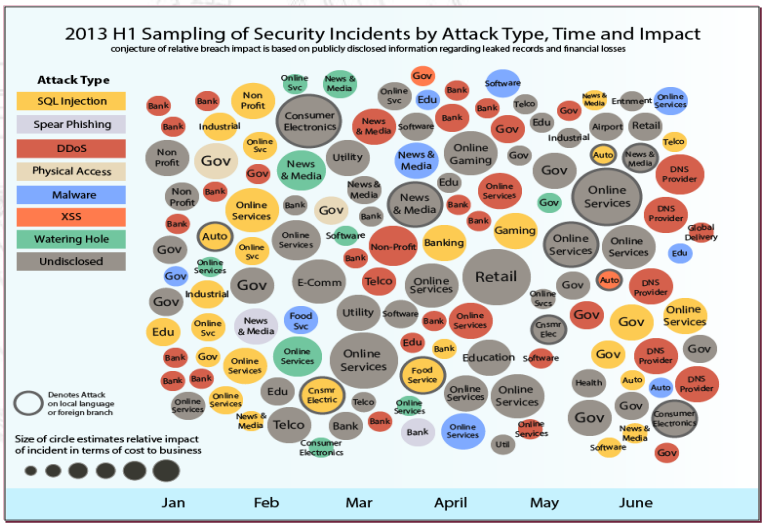
 Source : ENISA, 2011 : Botnets : Detection, Measurement, ...

Botnet History



 Source : RAND, Market for CyberCrime, 2014

Doesn't impact your business?

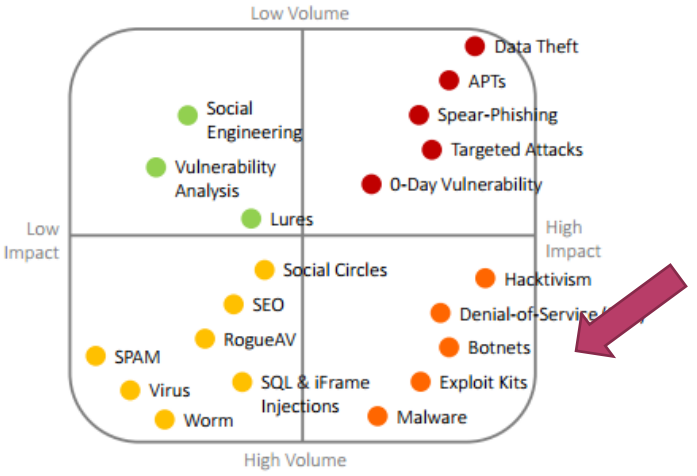


Source : IBM, X-Force Trends Report 09/2013

Attribution : top causes of data breaches 2012

Source : ISTR, October 2013, www.lsec.be

But who cares? – Business ? – not really



Source : LSEC, Innovations, Websense, 09/13

Should we even care?

Source : LSEC ACDC, Cyberdefcon March 2013

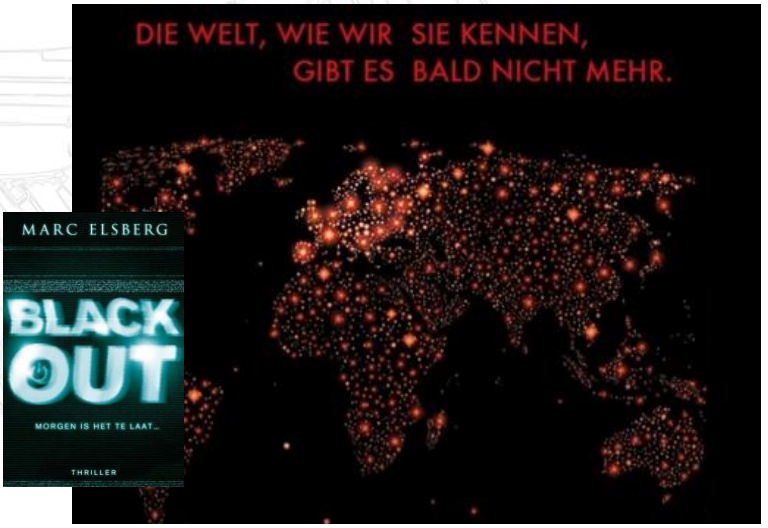
Carna Botnet : 420.000 bots – a research project

60k virus on an infected device:

- **Open a port for remote access by the central internet mapping systems.**
- **Reach out to scan and record details about a subset of the rest of the internet.**
- **Identify routers with telnet open onto the internet and a weak root password, e.g. root:root, admin:admin or either account with no password.**
- **Login and install the virus on the next open router in the ever-growing tree of zombies.**
- **For research purposes!**

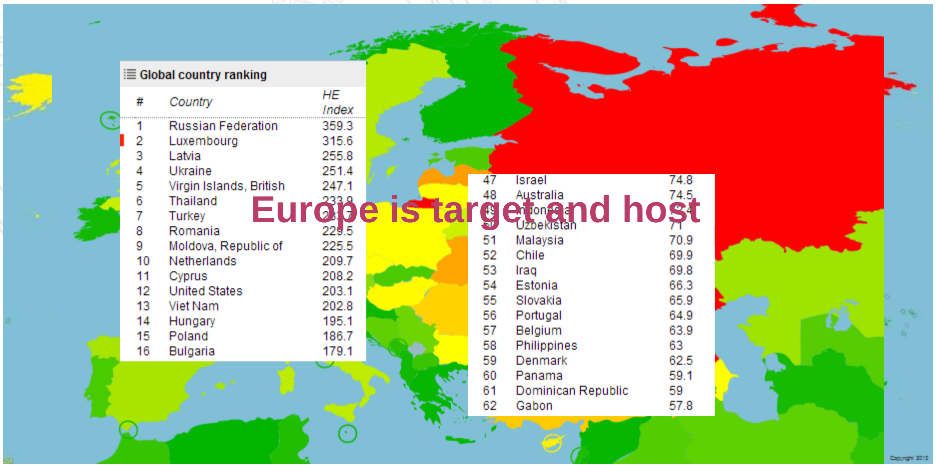
Source : LSEC, ACDC, Cyberdefcon 03/2013

The point?



Source : Marc Elsberg, Blackout, 2013

Relevance for ETSI Members : Global Threat Map Today



#	Country	HE Index
1	Russian Federation	359.3
2	Luxembourg	315.6
3	Latvia	255.8
4	Ukraine	251.4
5	Virgin Islands, British	247.1
6	Thailand	233.9
7	Turkey	[illegible]
8	Romania	229.5
9	Moldova, Republic of	225.5
10	Netherlands	209.7
11	Cyprus	208.2
12	United States	203.1
13	Viet Nam	202.8
14	Hungary	195.1
15	Poland	186.7
16	Bulgaria	179.1

47	Israel	74.8
48	Australia	74.5
49	[illegible]	[illegible]
[illegible]	Uzbekistan	71
51	Malaysia	70.9
52	Chile	69.9
53	Iraq	69.8
54	Estonia	66.3
55	Slovakia	65.9
56	Portugal	64.9
57	Belgium	63.9
58	Philippines	63
59	Denmark	62.5
60	Panama	59.1
61	Dominican Republic	59
62	Gabon	57.8

Europe is target and host

© Leaders in Security – LSEC, 2014, for ACDC – public , p 11

Source : Hostexploit, September 2013

Relevance to ETSI Members : Global Threat Map Today

HE Rank	HE Index	ASN	Name	Country	IPs
1	252.33	33182	HostDime.com, Inc.	US	63,232
2	249.28	26347	New Dream Network, LLC	US	230,656
3	243.51	11042	Landis Holdings Inc	US	28,416
4	226.75	27823	Dattatec.com	AR	8,192
5	220.57	29073	Ecatel Network	NL	13,312
6	219.59	8972	Intergenia AG	DE	149,760
7	213.56	31034	Aruba S.p.A.	IT	145,664
8	201.20	43146	Agava Ltd.	RU	19,712
9	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
10	195.66	40034	Confluence Networks Inc	VG	12,288
11	[illegible]	[illegible]	[illegible]	[illegible]	11,008
12	193.03	25532	Masterhost	RU	77,824
13	191.61	12824	home.pl	PL	204,800
14	184.51	34619	Cizgi Telekomunikasyon	TR	30,208
15	183.00	29182	ISPsystem	RU	44,288
16	178.01	30633	Leaseweb USA	US	14,592
17	174.69	46606	Unified Layer	US	508,416
18	162.44	26496	GoDaddy.com, LLC	US	1,636,352
19	162.05	39743	Voxility S.R.L.	RO	55,808
20	156.79	16276	OVH Systems	FR	1,170,944

Highest observed concentrations of malicious activity

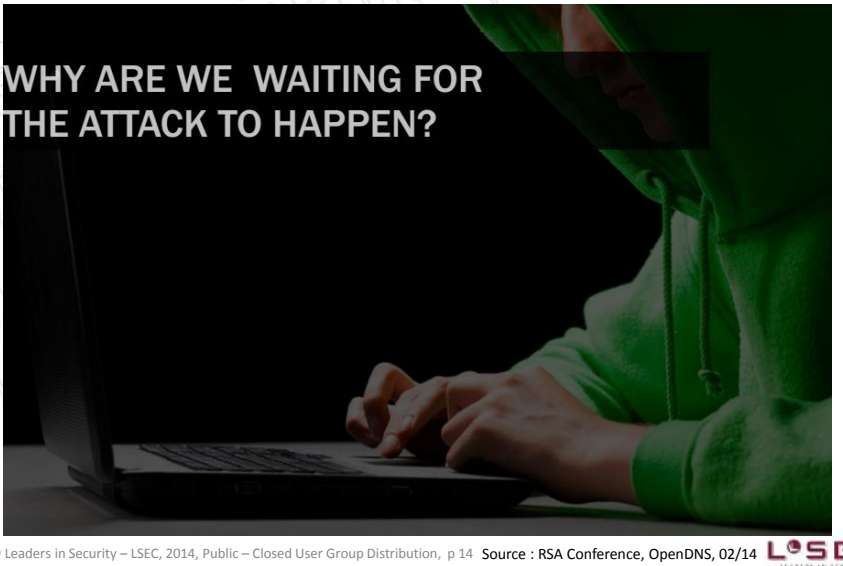
© Leaders in Security – LSEC, 2014, for ACDC – public , p 12

Source : Hostexploit, September 2013

Botnet Relevance for Business

 Source : various, GoDaddy, Checkpoint

Change in attitude



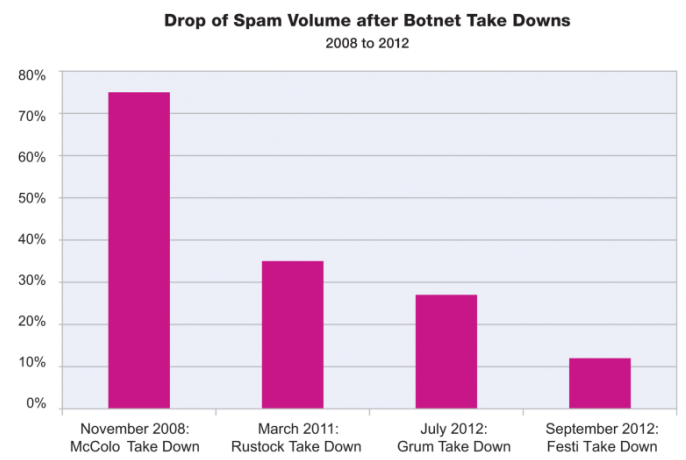
 Source : RSA Conference, OpenDNS, 02/14

So Let's Mitigate

	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	*	*		*

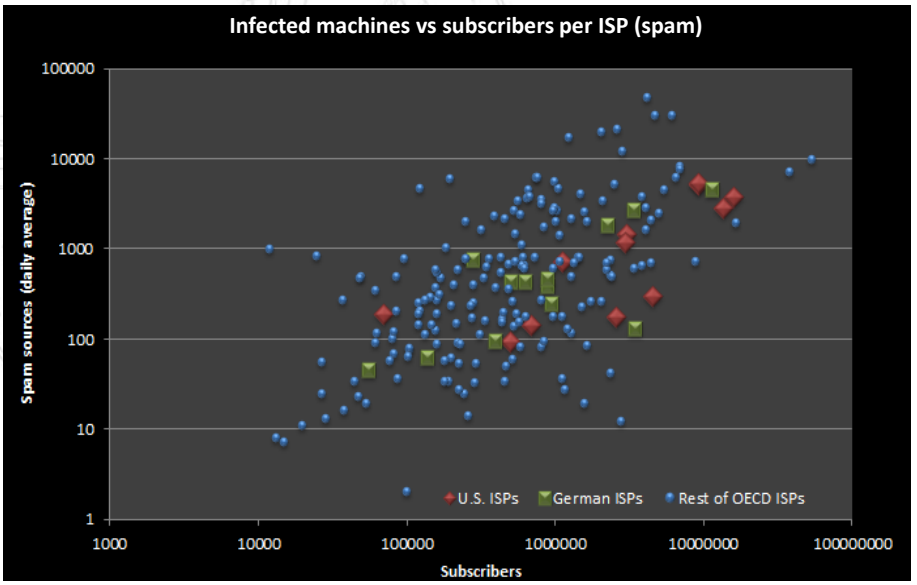
 Source : ENISA, 2012 : DG INFSO CIP PSP 15

Impact of Botnet Defense



Source: IBM X-Force® Research and Development

 Source : PCWorld, IBM



 Source : Botnet mitigation and the role of ISPs, TU Delft, March 2013

European Commission

ACDC
&
The European Commission's
Cyber Security Strategy

Trust and Security
DG CONNECT - European Commission

Cybersecurity the need for further EU action

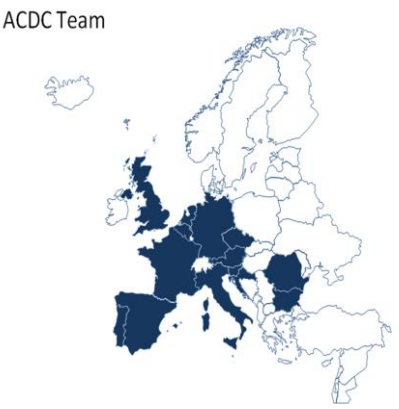
1. Economic and social benefits of the Digital Single Market
2. Risks and incidents on the rise > Lack of trust, economic losses, missed opportunities
3. Cross-border nature of risks and incidents
4. Insufficient national preparedness and cooperation across the EU

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

28 partners – 14 member countries

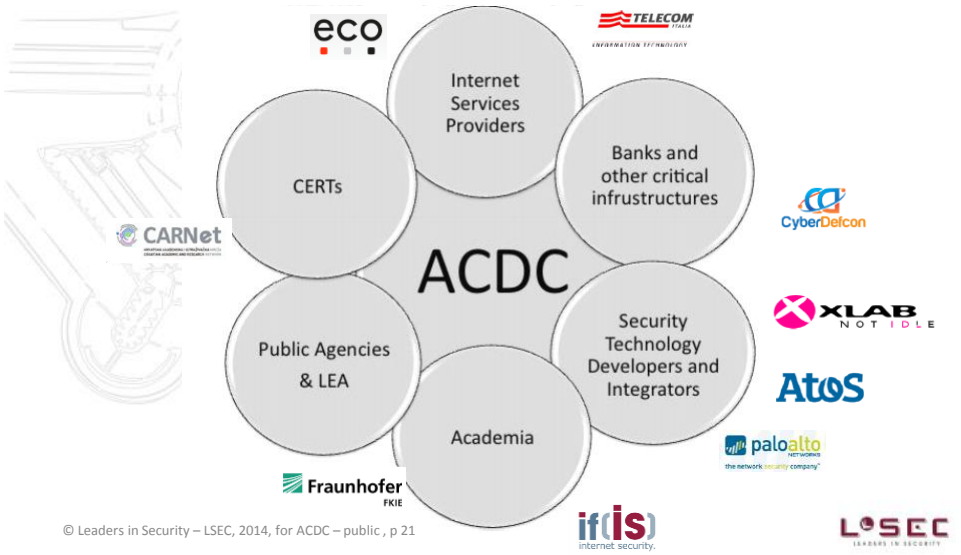
ECO Association of the German Internet Industry
Technikon Forschungs- und Planungsgesellschaft mbH
Atos Spain S.A
Bulgarian Posts PLC
Croatian Academic and Research Network - CARNet and Croatian National CERT
Romanian National Computer Emergency Response Team - CERT-RO & Romanian Partners
Cognitive Security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



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

20

Consortium Structure



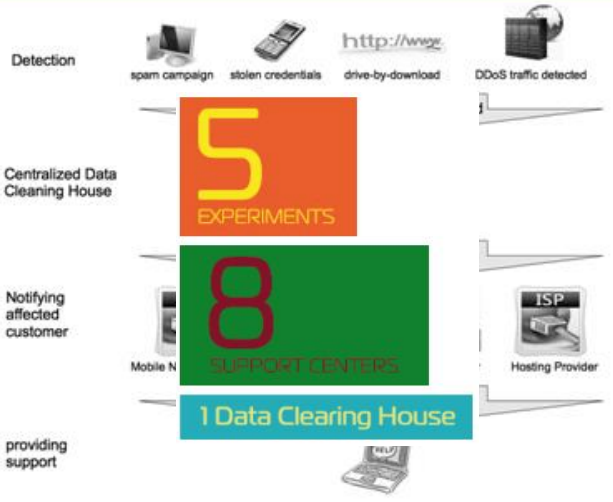
EC Botnet Fighting Team

 Source : ACDC Kickoff Meeting, DE-CIX, Frankfurt, 2013 22

Pan-European Approach

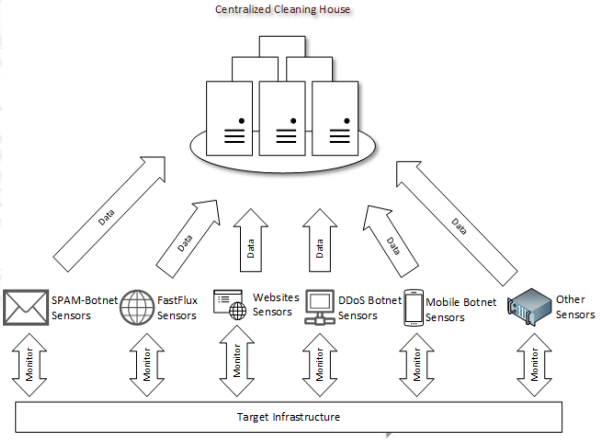
- extensive **sharing of information** – without boarders:
  → across networks & member states
- provide a complete set of **solutions**:
  → accessible online for mitigating on-going attacks
- use the **pool of knowledge**
  → to create best practices
  → to support affected end customers & organisations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

Solution

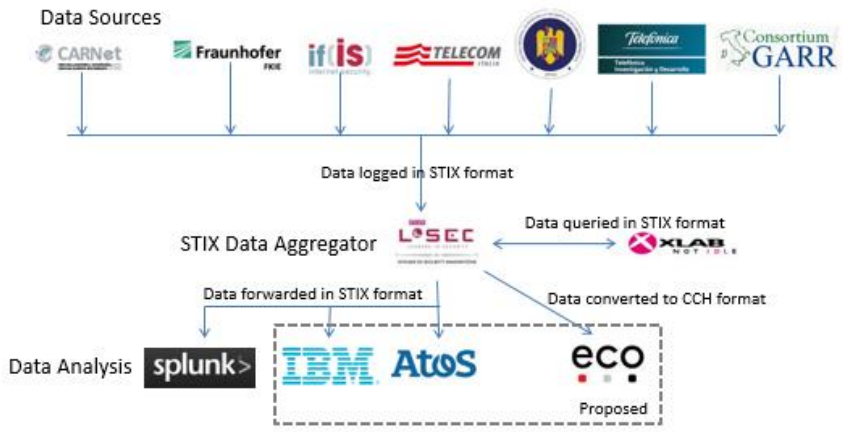


Tool Set

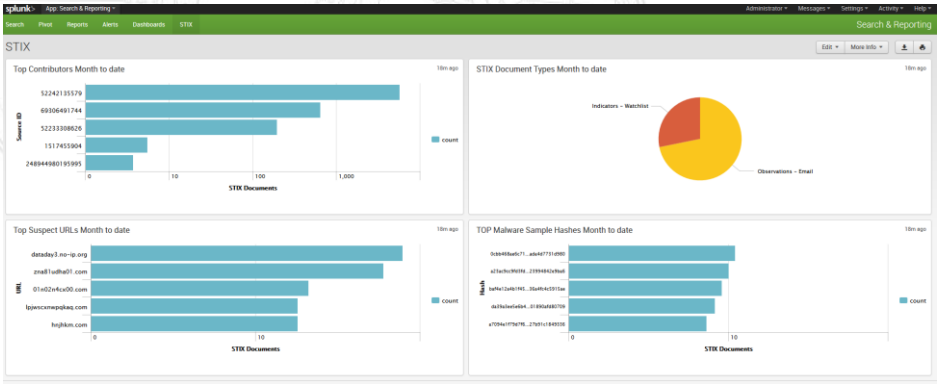
From Detection to Protection



STIX Aggregator

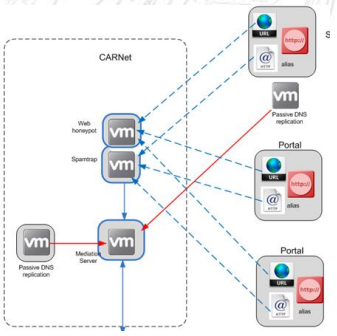


Types of Information Currently Collected



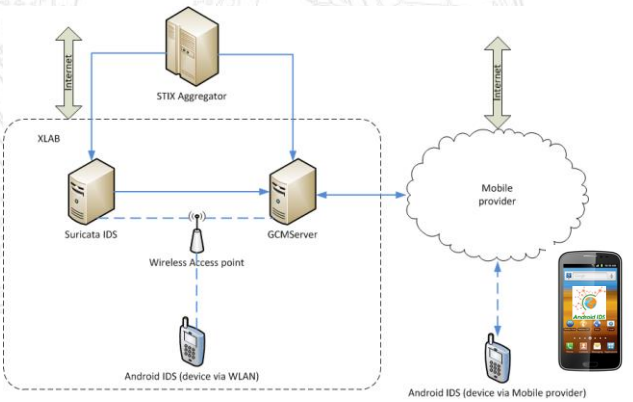
Operational Detection

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



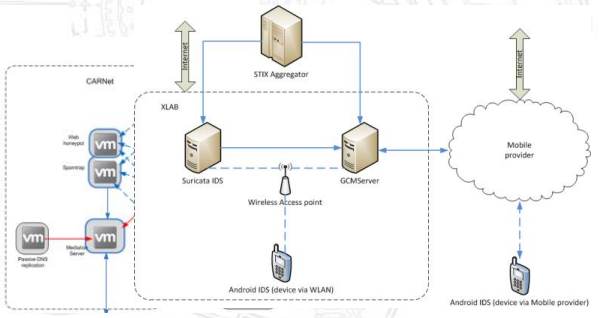
Operational Detection

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



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.

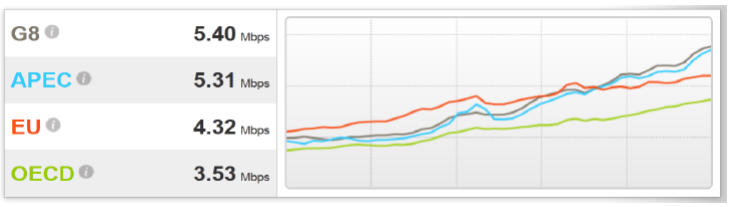
Types of Information Currently Collected

- 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.

Future Analysis

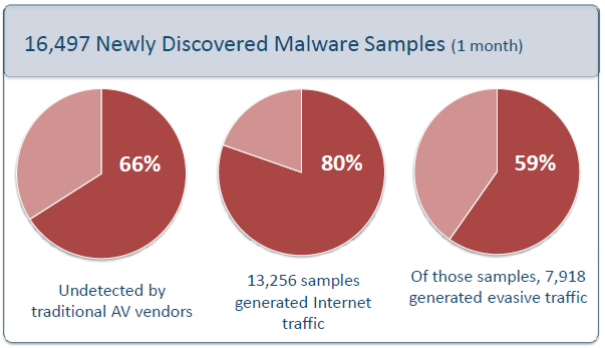
Every bot has about 5 Mbps upload bandwidth



(and about 12 Mbps download bandwidth, too)

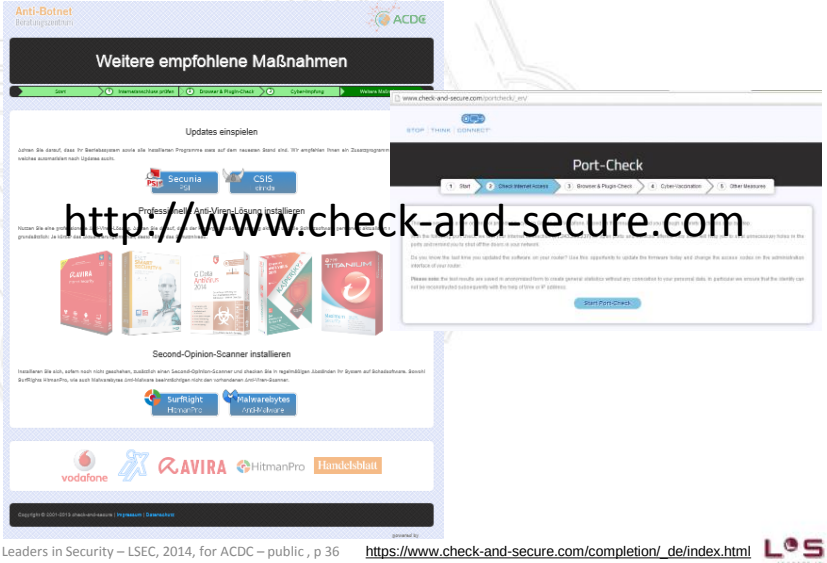
Source : IFIS, January 2013

Other Sensors & Impact



 Source : Palo Alto March 2013

User Tools & impact



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

 https://www.check-and-secure.com/completion/_de/index.html

User Tools & Impact

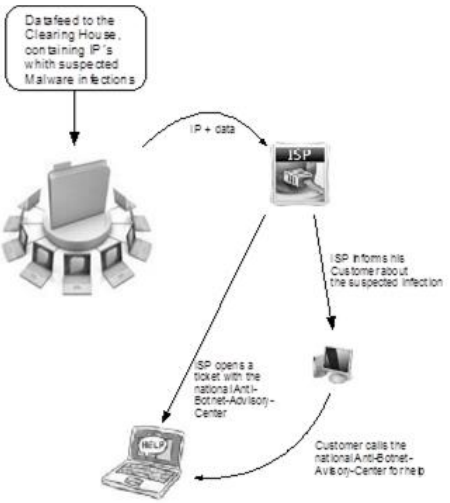
https://www.initiative-s.de/de/index.html

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

Sharing Impact

 http://stix.mitre.org/

Organization & User Impact



Support Centers

www.botvrij.be
antibot.hr
www.botfrei.de

40

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 - Deployment
3. Data & Intelligence Sharing
4. Awareness Creation
5. Influencing Policy

NOT THE END

More information and follow-up

www.acdc-project.eu
www.botfree.eu

Q or C
Ulrich Seldeslachts
ulrich@lsec.be
+32 475 71 3602

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
- **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
- **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