

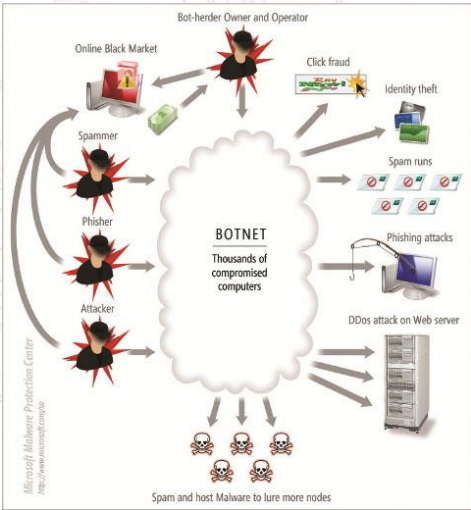


Advanced Cyber Defense Center ACDC
European Anti Botnet Pilot Action
Annual GI/ACM & EU Club R2Gs - ETSI ISG ISI
May 14, 2014

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



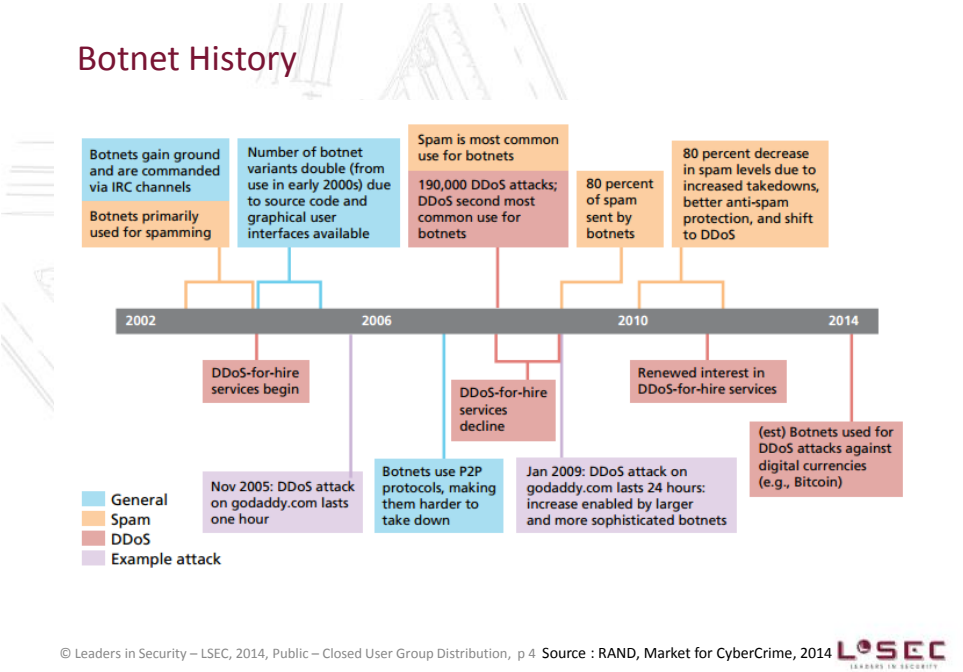
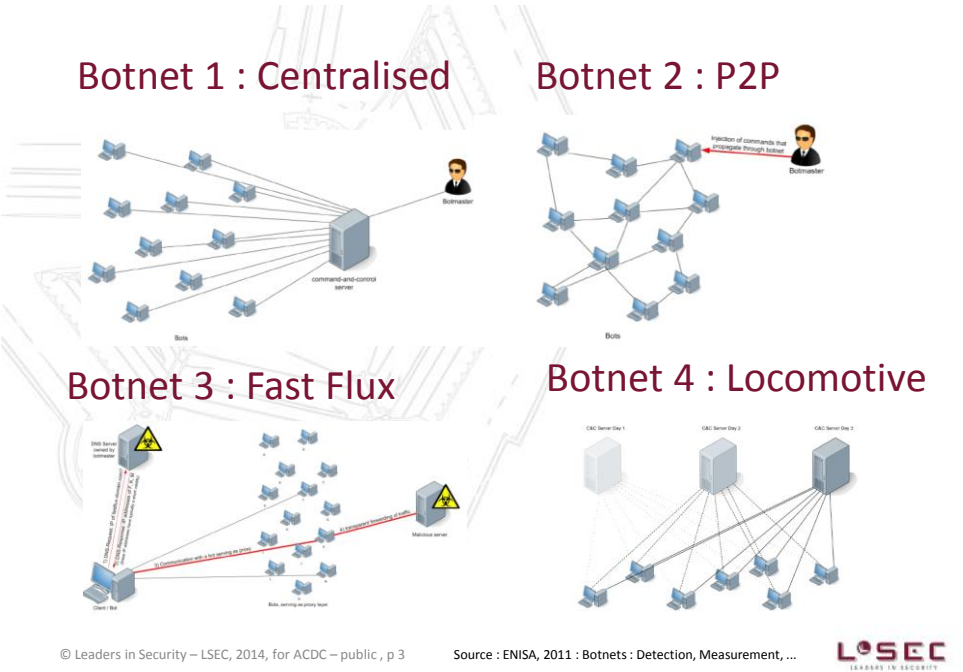
What Botnets do



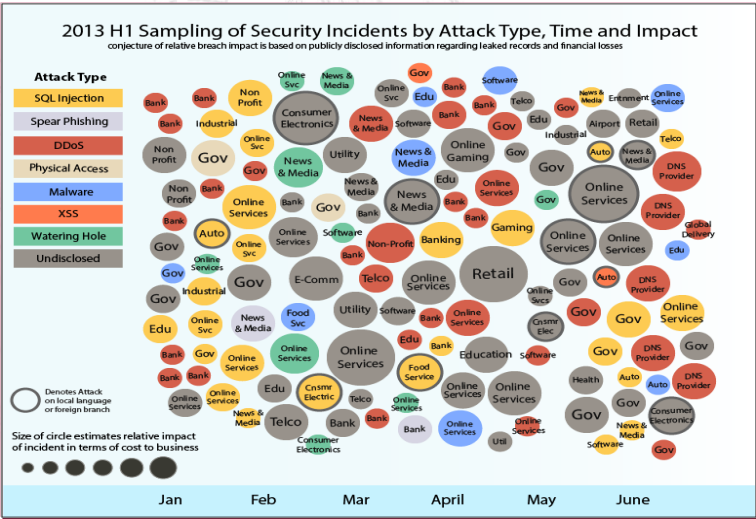
© Leaders in Security – LSEC, 2014, for ACDC – public, p 2

Source : PCWorld





Doesn't impact your business?

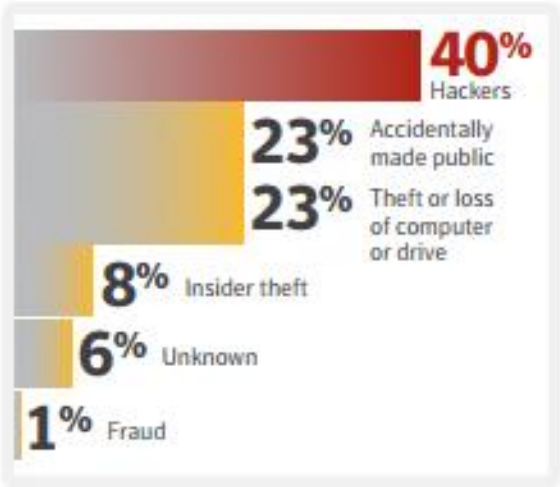


© Leaders in Security – LSEC, 2014, Public, p 5

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

LSEC
LEADERS IN SECURITY

Attribution : top causes of data breaches 2012

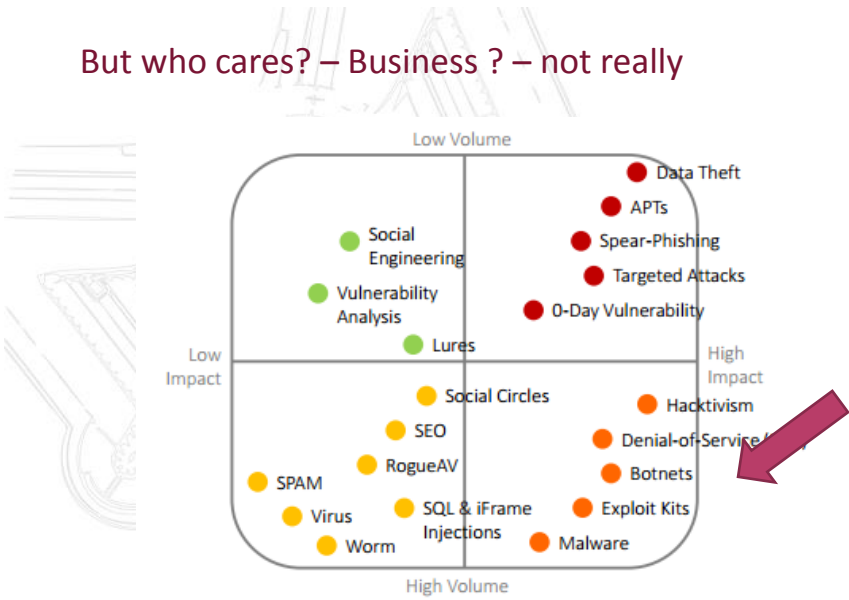


© Leaders in Security – LSEC, 2014, Public, p 6

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

LSEC
LEADERS IN SECURITY

But who cares? – Business ? – not really



© Leaders in Security – LSEC, 2014, for ACDC – public , p 7

Source : LSEC, Innovations, Websense, 09/13

LSEC
LEADERS IN SECURITY

Should we even care?

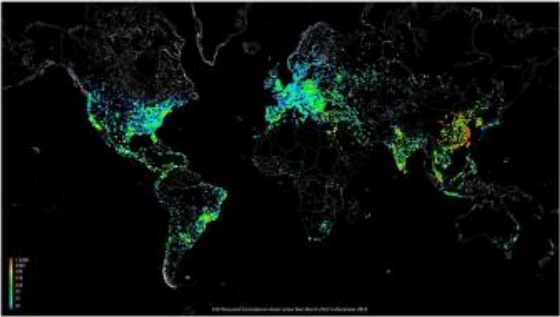


© Leaders in Security – LSEC, 2014, for ACDC – public , p 8

Source : LSEC ACDC, Cyberdefcon March 2013

LSEC
LEADERS IN SECURITY

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!

© Leaders in Security – LSEC, 2014, for ACDC – public , p 9

Source : LSEC, ACDC, Cyberdefcon 03/2013




The point?

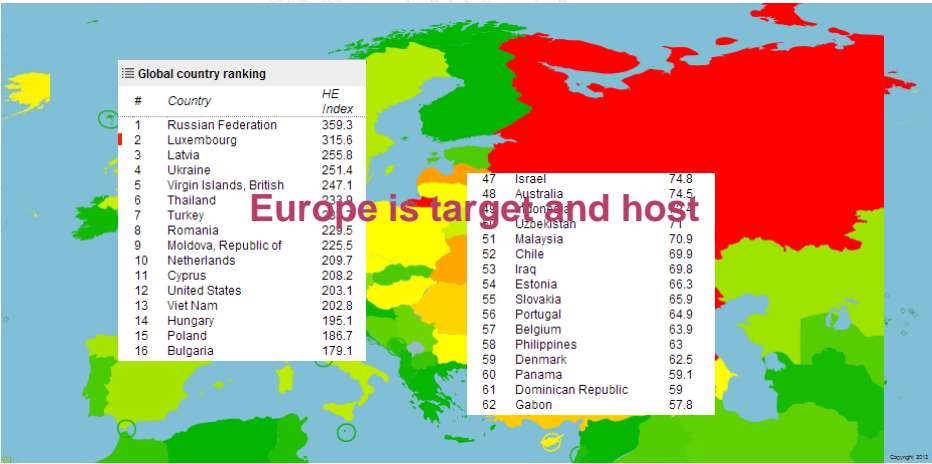


© Leaders in Security – LSEC, 2014, for ACDC – public , p 10

Source : Marc Elsberg, Blackout, 2013



Relevance for ETSI Members : Global Threat Map Today



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

Source : Hostexploit, September 2013

LSEC
LEADERS IN SECURITY

Relevance to ETSI Members : Global Threat Map Today

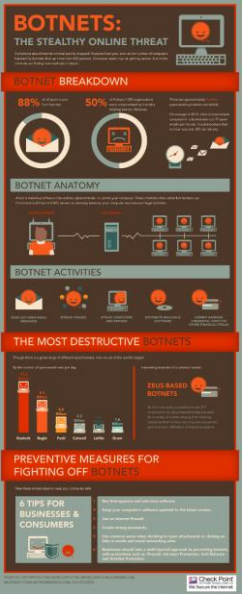


© Leaders in Security – LSEC, 2014, for ACDC – public , p 12

Source : Hostexploit, September 2013

LSEC
LEADERS IN SECURITY

Botnet Relevance for Business



BOTNETS: THE STEALTHY ONLINE THREAT

BOTNETS BREAKDOWN

- 88% of botnets are used for spamming
- 50% of botnets are used for DDoS attacks

BOTNET ANATOMY

Botnets are made up of thousands of infected computers, known as bots, which are controlled by a central command and control server. The bots can be used to perform a variety of tasks, such as sending spam, launching DDoS attacks, and stealing data.

BOTNET ACTIVITIES

- Spamming
- DDoS attacks
- Phishing
- Malware distribution
- Stolen data

THE MOST DESTRUCTIVE BOTNETS

Botnets are a significant threat to businesses and consumers. They can be used to launch DDoS attacks, steal data, and spread malware. The most destructive botnets are those that are used for DDoS attacks, as they can cause significant damage to businesses and consumers.

PREVENTIVE MEASURES FOR FIGHTING OFF BOTNETS

There are several steps that businesses and consumers can take to protect themselves from botnets:

- Keep software up to date
- Use strong passwords
- Be cautious of phishing emails
- Use antivirus software
- Be cautious of downloading files from the internet

6 TIPS FOR BUSINESSES & CONSUMERS

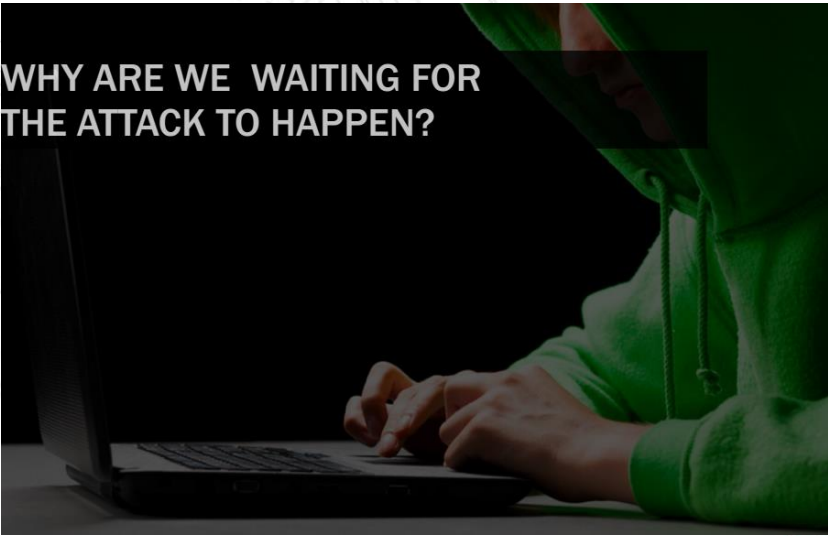
- 1. Keep software up to date
- 2. Use strong passwords
- 3. Be cautious of phishing emails
- 4. Use antivirus software
- 5. Be cautious of downloading files from the internet
- 6. Report suspicious activity to the authorities

© Leaders in Security – LSEC, 2014, for ACDC – public, p 13

Source : various, GoDaddy, Checkpoint




Change in attitude



© Leaders in Security – LSEC, 2014, Public – Closed User Group Distribution, p 14

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	*	*		*

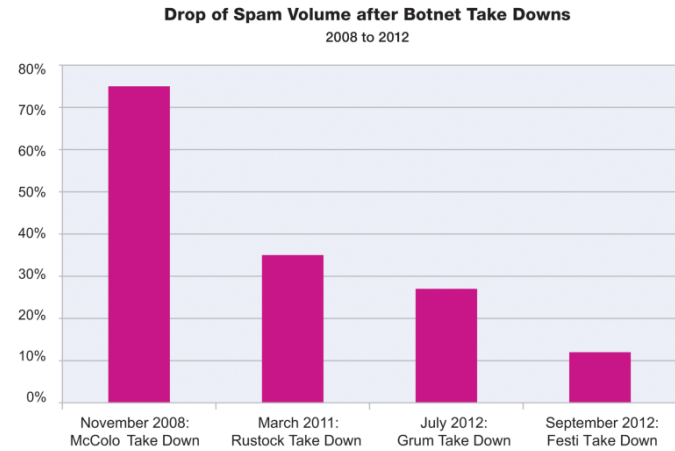
© Leaders in Security – LSEC, 2014, for ACDC – public , p 15

Source : ENISA, 2012 : DG INFSO CIP PSP

15

LSEC
LEADERS IN SECURITY

Impact of Botnet Defense

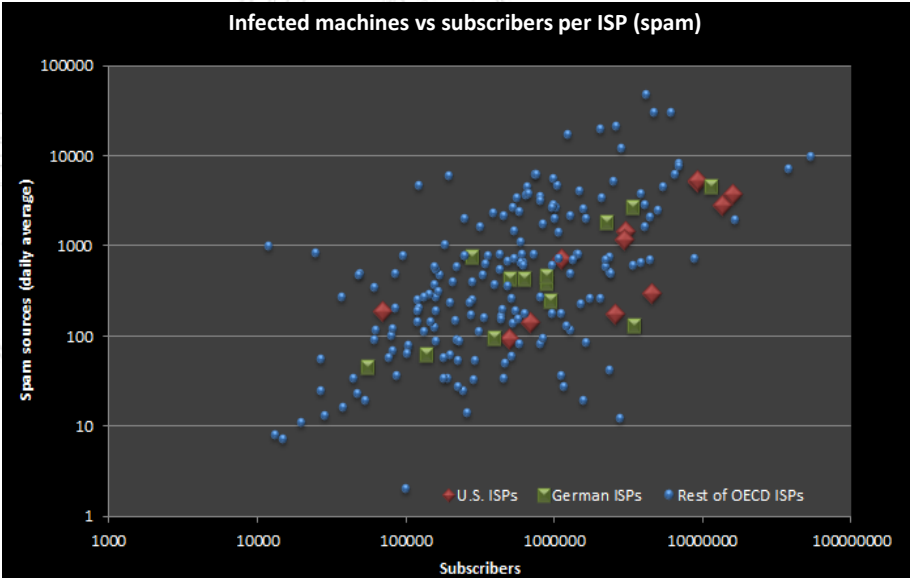


© Leaders in Security – LSEC, 2014, for ACDC – public , p 16

Source: IBM X-Force® Research and Development

Source : PCWorld, IBM

LSEC
LEADERS IN SECURITY



© Leaders in Security – LSEC, 2014, for ACDC – public , p 17 Source : Botnet mitigation and the role of ISPs, TU Delft, March 2013

LSEC
LEADERS IN SECURITY



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

© Leaders in Security – LSEC, 2014, for ACDC – public , p 19






28 partners – 14 member countries



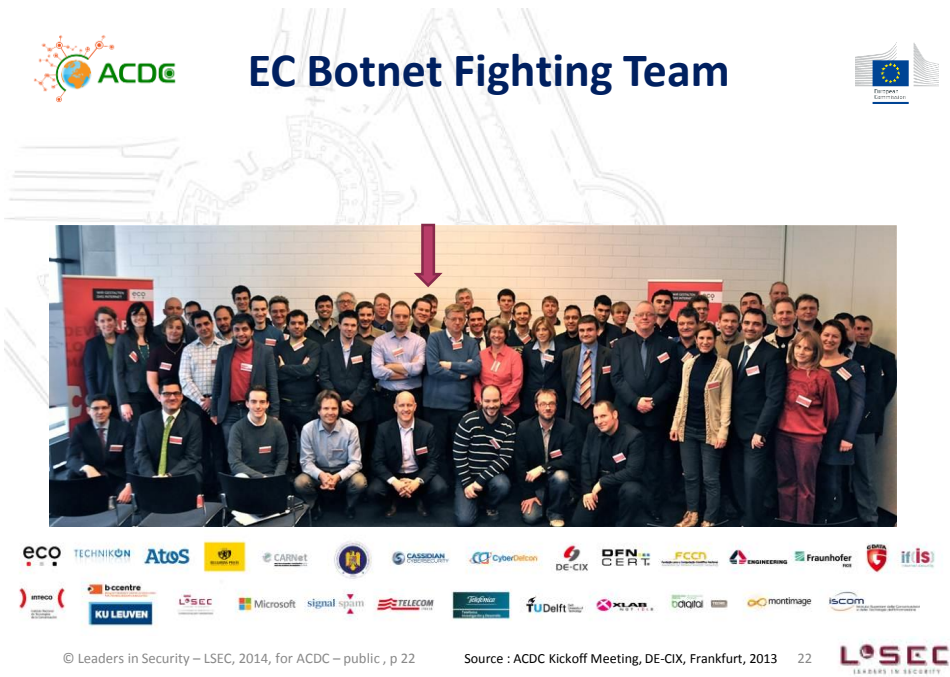
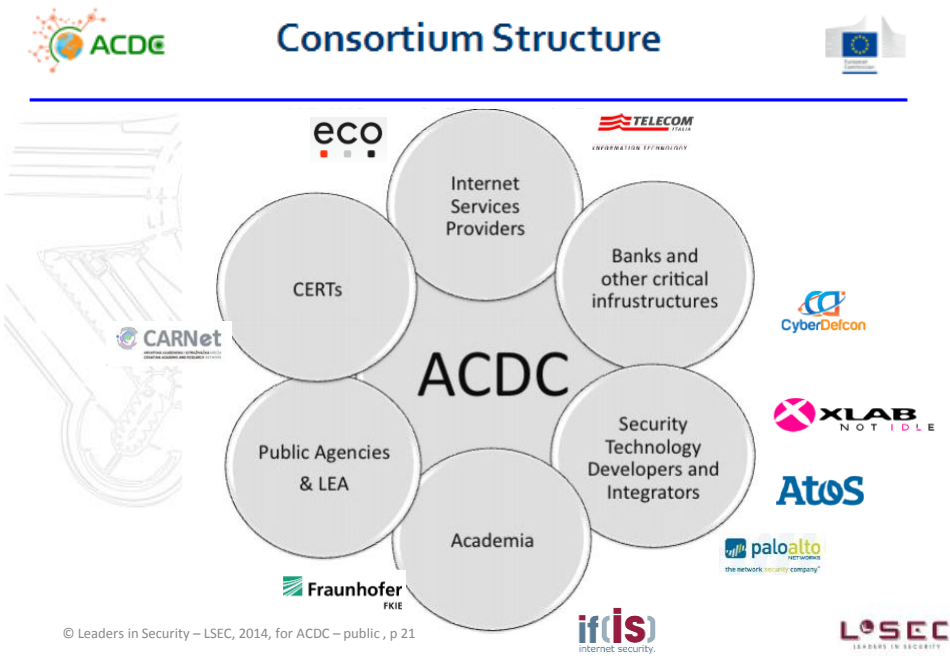
ECO Association of the German Internet Industry
Technikon Forschungs- und Planungsgesellschaft mbH
Atos Spain S.A
Bulgarian Posts PLC
Croatian Academic and Research Network - CARNet and Croatian National CERT
Romanian National Computer Emergency Response Team - CERT-RO & Romanian Partners
Cognitive Security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

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, 2014, for ACDC – public , p 20





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, 2014, for ACDC – public , p 23



Solution



The diagram illustrates a four-stage cyber defense solution flow:

- Detection:** Includes icons for a laptop, a mobile phone, a URL (<http://www>), and a server. Specific threats listed are "spam campaign", "stolen credentials", "drive-by-download", and "DDoS traffic detected".
- Centralized Data Cleaning House:** Represented by an orange box with a large yellow number "5" and the word "EXPERIMENTS".
- Notifying affected customer:** Includes icons for a mobile phone and a server. A label "Mobile N" is present.
- providing support:** Represented by a green box with a large red number "8" and the words "SUPPORT CENTERS". Below this is a blue box labeled "1 Data Clearing House".

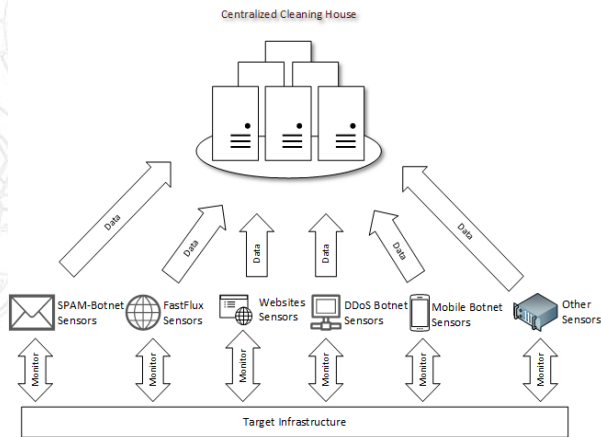
Additional components shown on the right include an "ISP" (Internet Service Provider) and a "Hosting Provider".

© Leaders in Security – LSEC, 2014, for ACDC – public , p 24



Tool Set

From Detection to Protection

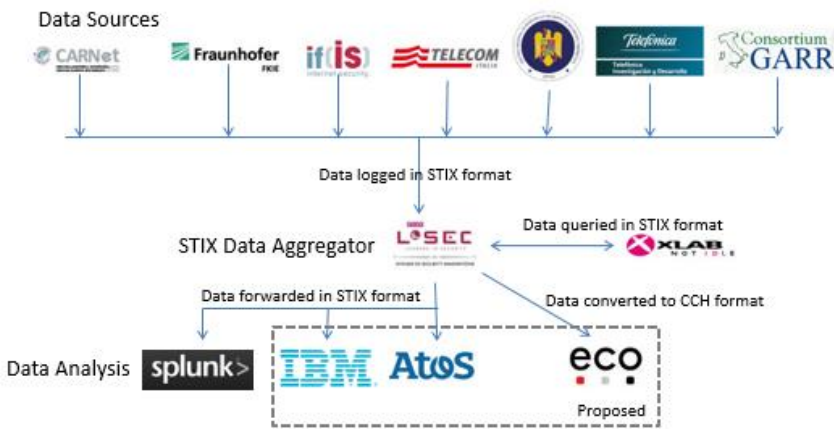


© Leaders in Security – LSEC, 2014, for ACDC – public, p 25

25 **LSEC**
LEADERS IN SECURITY




STIX Aggregator




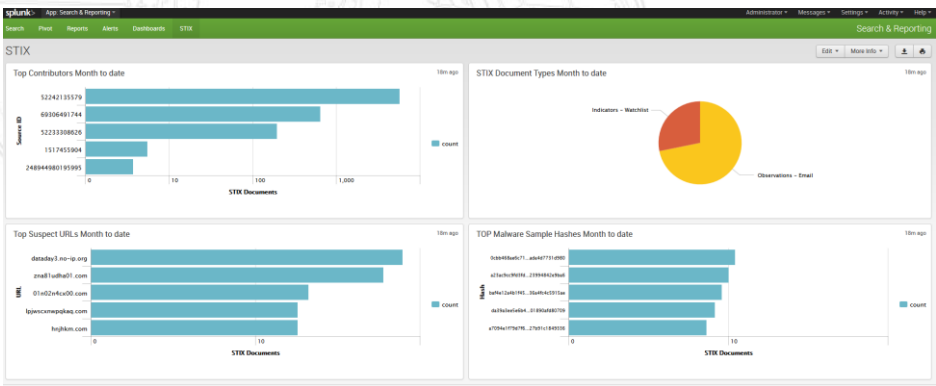
© Leaders in Security – LSEC, 2014, for ACDC – public, p 26

LSEC
LEADERS IN SECURITY





Types of Information Currently Collected






© Leaders in Security – LSEC, 2014, for ACDC – public , p 27

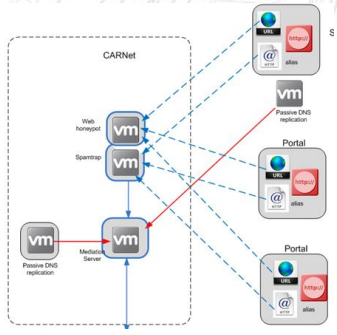
27 




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, 2014, for ACDC – public , p 28


28 

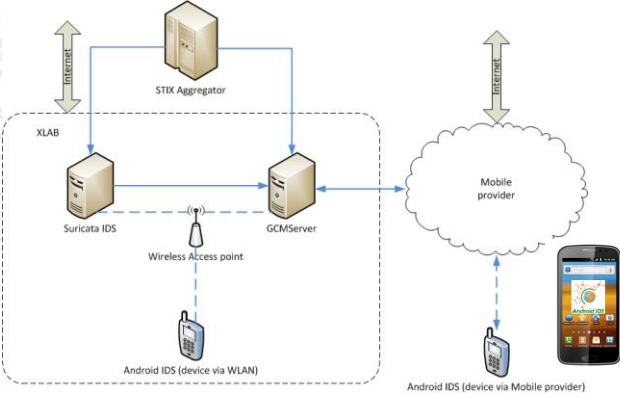


Operational Detection




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







The diagram illustrates the Operational Detection architecture. It shows a central dashed box containing the XLAB infrastructure, which includes a Suricata IDS, a GCM Server, and a Wireless Access point. An Android IDS device is connected to the Wireless Access point via WLAN. The XLAB infrastructure is connected to an STIX Aggregator and a Mobile provider. The STIX Aggregator is connected to the Internet. The Mobile provider is connected to the Internet and provides service to an Android phone. The Android phone is also connected to the Internet.

© Leaders in Security – LSEC, 2014, for ACDC – public , p 29


29 

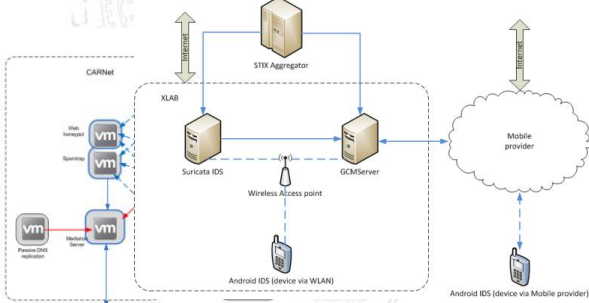


Data Sharing & Analysis




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






The diagram illustrates the Data Sharing & Analysis architecture. It shows a central dashed box containing the XLAB infrastructure, which includes a Suricata IDS, a GCM Server, and a Wireless Access point. An Android IDS device is connected to the Wireless Access point via WLAN. The XLAB infrastructure is connected to an STIX Aggregator and a Mobile provider. The STIX Aggregator is connected to the Internet. The Mobile provider is connected to the Internet and provides service to an Android phone. The Android phone is also connected to the Internet. The STIX Aggregator is connected to the Internet. The Mobile provider is connected to the Internet and provides service to an Android phone. The Android phone is also connected to the Internet.


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




STIX Aggregator




URL Checker
The specified URL was classified as dangerous.




© Leaders in Security – LSEC, 2014, for ACDC – public , p 30

30 




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.

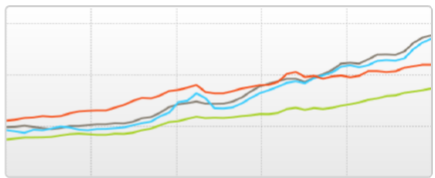


Future Analysis

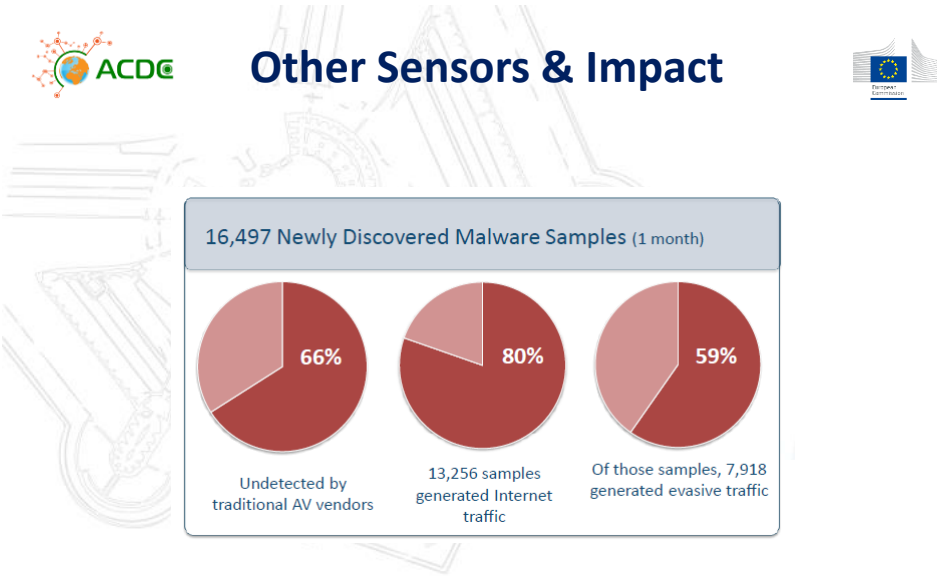


Every bot has about 5 Mbps upload bandwidth

G8	5.40 Mbps
APEC	5.31 Mbps
EU	4.32 Mbps
OECD	3.53 Mbps




(and about 12 Mbps download bandwidth, too)

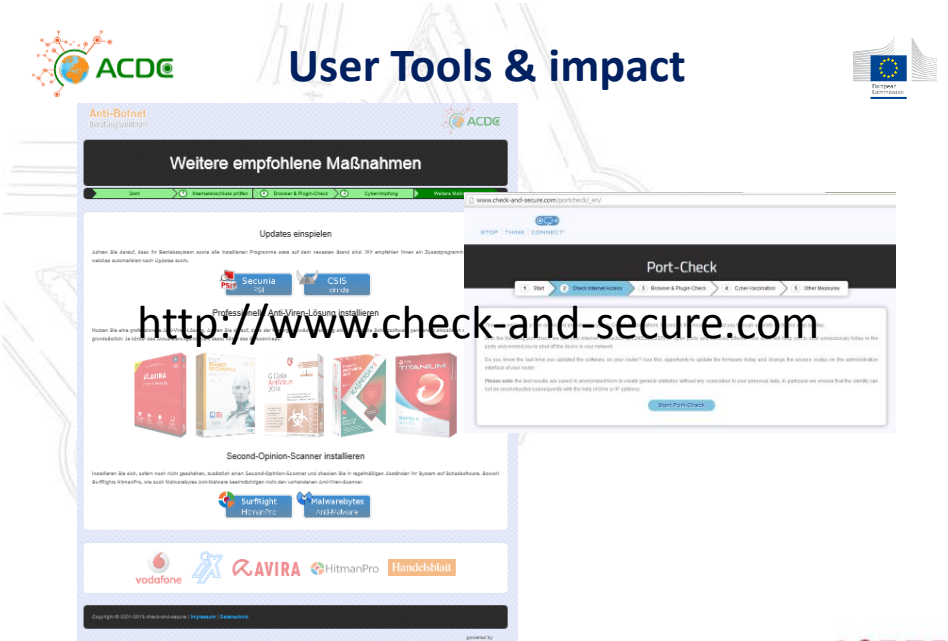


© Leaders in Security – LSEC, 2014, for ACDC – public , p 35

Source : Palo Alto March 2013

35





© Leaders in Security – LSEC, 2014, for ACDC – public , p 36

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





User Tools & Impact



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

INITIATIVE S

Startseite

Schützen

Säubern

Über das Projekt

Teilnehmer

Kontakt

Eine Initiative von

eco

Gefördert durch

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

Vorbeugen. Untersuchen. Sicherheit genießen.

Schützen Sie Ihren Webauftritt und Ihre Besucher vor unbemerkten Manipulationen und erhalten Sie professionelle Hilfe. Geben Sie hier den Namen Ihrer Internetadresse ein und registrieren Sie sich kostenlos.

domain-der-webseite.de

KOSTENFREI ANMELDEN

SEITENCHECK

SÄUBERN

SCHÜTZEN

Herzlich willkommen beim Seiten-Check der Initiative-S!

TASK FORCE IT-SICHERHEIT IN DER WIRTSCHAFT

© Leaders in Security – LSEC, 2014, for ACDC – public , p 37

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



Sharing Impact



THREAT STREAM

Booz | Allen | Hamilton

NORTHROP GRUMMAN

CYBERIQ

WORLD BANK

Bromium

GE

MANDIANT

Cyveillance

RED SKY ALLIANCE

USAA

FINANCIAL SERVICES

NATO

tripwire

REVERSING LABS

incidentiologic

MITRE

LOOKINGGLASS

JID

CERT

CROWDSTRIKE

US-CERT

LOCKHEED MARTIN

orange background.jpg

FOREGROUND SECURITY

REN-ISAC

DTCC

Critical Response

PUNCH

ERT-EU

STEGOSYSTEMS

ISIGHTPARTNERS

NCI Security LLC

VISA

NIST

GENERAL DYNAMICS

SIEMENS

verizon

6f4a8be3f316

19114:02:21.493909

CARNet Honeypot

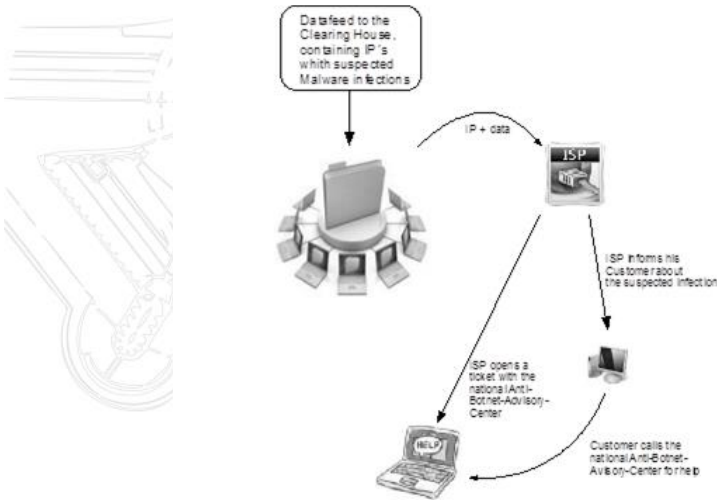
© Leaders in Security – LSEC, 2014, for ACDC – public , p 38

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





Organization & User Impact



© Leaders in Security – LSEC, 2014, for ACDC – public, p 39



Support Centers



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







© Leaders in Security – LSEC, 2014, for ACDC – public , p 41

41



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





© Leaders in Security – LSEC, 2014, for ACDC – public , p 42



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>

© Leaders in Security – LSEC, 2014, for ACDC – public, p 43

