LSEC

BRUCON ACDC Information Sharing Workshop

Ulrich Seldeslachts ,
Gent, September 27th, 2013

agentschap voor Innovatie door Wetenschap en Technologie

Disclaimer

I'm not a security expert, I don't want to be a security expert, but I want to understand to be able to explain. We address security issues to others and help you to make others understand that there are many security challenges and issues, to highlight some of them and to encourage people, organizations and institutions to do something about them. I don't know anything (or at least less than you) about botnets and I'm not planning to be an expert on them. Please make me understand how this works and where you could help us with.

About Information Sharing?

Hack victims urged to share the gory details

Advanced Cyber Security Center fosters voluntary information sharing among private organizations as a way of staying ahead of the bad guys

By Colin Neagle, Network World
September 12, 2013 11:45 AM ET

NSA Director: Information-Sharing Critical To U.S. Cybersecurity

2013/091213-hack

NSA Director and U.S. Cyber Command chief Gen. Keith Alexander discusses challenges to protecting U.S. interests in cyberspace

1 Comments | 20 Like | 131 Tweet | 4 +1 | 76 Share | Submit | 5 | Mail | Print

FOR COLLABORATION

...stry share information and

...ent-launches-

Brussels, 7.2.2013

DIRECTIVE ...
concerning mea...

SECURITY OF T...
AD

Brian Prince, Contributing Writer
Dark Reading March 29, 2013

Security requirements and incident notification

Member States shall ensure that public administrations and market operators notify to the competent authority incidents having a significant impact on the security of the core services they provide.

http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf

Sharing the Wealth, and the Burdens, of Threat Intelligence

Information Sharing?

IODEF-extension for structured cybersecurity information

their likeness.
nd, and mitigates threats
ions

http://www.verizonenterprise.com/resources/whitepapers/wp_verizon-incident-sharing-metrics-framework_en_xg.pdf

Information Sharing

STIX™

Effective Cyber Threat Intelligence and Information Sharing

http://stix.mitre.org/

Information Sharing?

STIX™

Language

Specify **Capture** **Characterize** **Communicate**

Cyber Threat Information

Community-driven

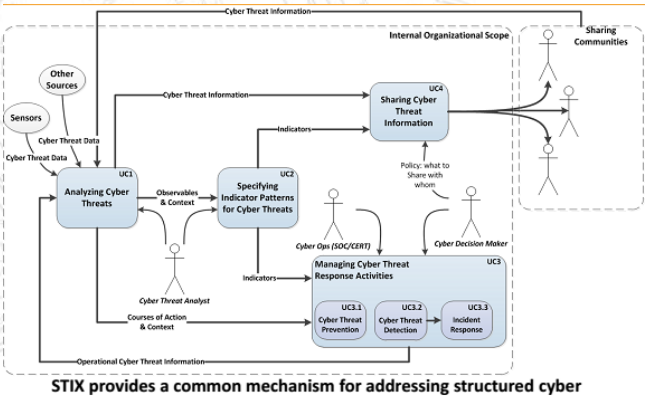
Consistency **Clarity** **Support automation**

http://stix.mitre.org/

Information Sharing?

STIX™

TAXII™ Trusted Automated eXchange of Indicator Information



STIX provides a common mechanism for addressing structured cyber threat information across and among this full range of use cases improving consistency, efficiency, interoperability, and overall situational awareness.

http://stix.mitre.org/

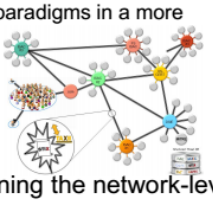
LSEC LEADERS IN SECURITY

Information Sharing?

STIX™

TAXII™ Trusted Automated eXchange of Indicator Information

- Trusted Automated eXchange of Indicator Information
- The goal of TAXII is to facilitate the exchange of structured cyber threat information
  - Designed to support existing sharing paradigms in a more automated manner



- TAXII is a set of specifications defining the network-level activity of the exchange
  - Defines services and messages to exchange data
  - Does NOT dictate *HOW* data is handled in the back-end, *WHAT* data is shared or *WHO* it is shared with
  - TAXII is NOT a sharing program

http://stix.mitre.org/

LSEC LEADERS IN SECURITY

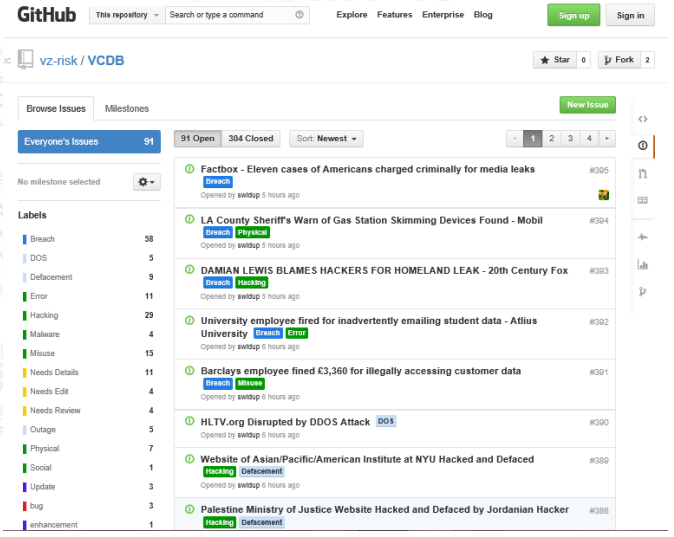
Information Sharing?

Consider these questions:

- What activity are we seeing? — Observable
- What threats should I look for on my networks and systems and why? — Indicator
- Where has this threat been seen? — Incident
- What does it do? — TTP
- What weaknesses does this threat exploit? — ExploitTarget
- Why does it do this? — Campaign
- Who is responsible for this threat? — ThreatActor
- What can I do about it? — Course of Action

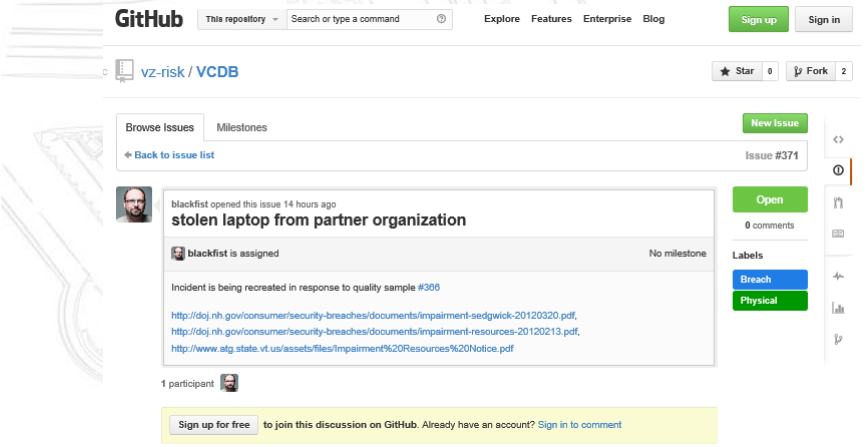
http://stix.mitre.org/

Information Sharing?



https://github.com/vz-risk/VCDB/issues

Information Sharing?



https://github.com/vz-risk/VCDB/issues/371

Information Sharing?

1. Identifying attack factors
    1. "CiSP has recognised trends within certain groups of attackers and the means by which they infiltrate their victims"
    2. Spear phishing emails continue to persist using topical subjects as a means to fool recipients into opening the email and clicking on the malicious contents.
    3. Multiple members have been able to share the information they have gathered, posts enriched, providing additional means of prevention for other members in the form of indicators, and attribution to a recognised attack group.
2. capability to provide actionable intelligence
3. Operational services such as risk mitigation, incident response, and information sharing
4. Fast response on accurate, actionable and relevant information
5. Empower business resiliency through security planning, disaster response and recovery execution.

Objective

1. Share knowledge on info-sharing models, methodologies, best practices
2. Find info-sharing partners, learn from market experiences
3. Develop info sharing platform in Belgium – build support centers
4. Engage potential members
5. Find barriers to entry and capabilities
6. Find additional resources to moderate platforms and provide

Creating Security Awareness

1. Publications
2. Seminars, Conferences, Workshops
3. International representation

About LSEC : Thought Leadership



About LSEC : ACD Project & information sharing

ACDC

Advanced Cyber Defence Center

I

anti-botnet pilot project

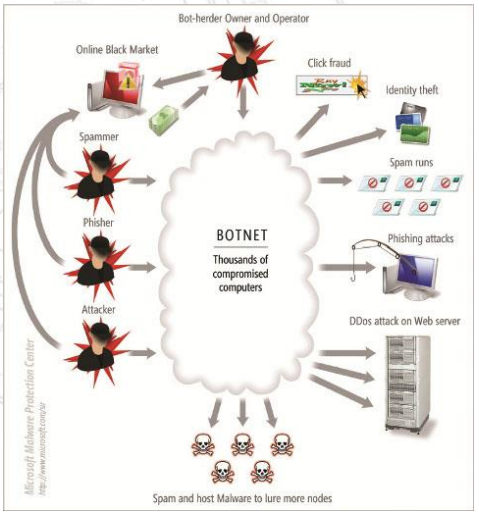
LSEC

European Commission

ACDC
&
The European Commission's
Cyber Security Strategy

Trust and Security
DG CONNECT - European Commission

What Botnets do



Source : PCWorld

Fragmented response

	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

28 partners – 14 member countries

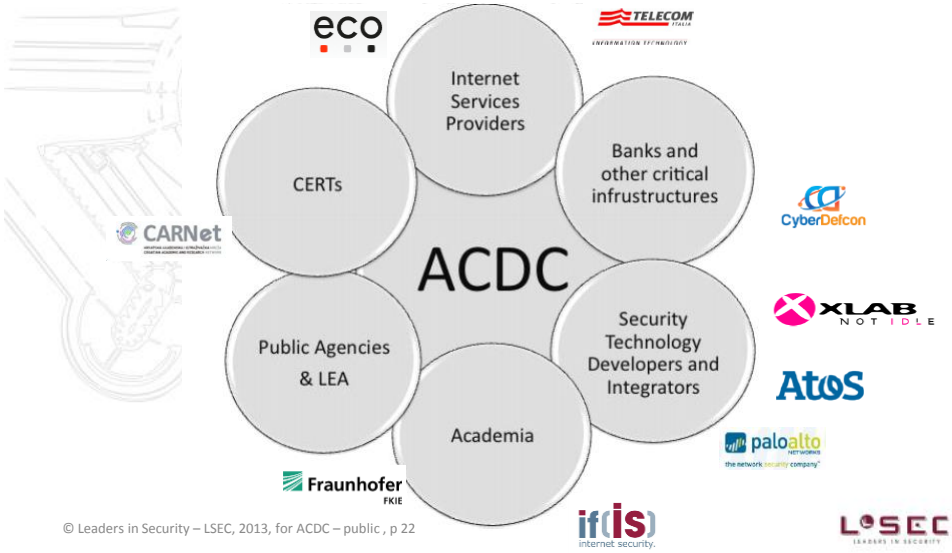
ECO Association of the German Internet Industry
Technikon Forschungs- und Planungsgesellschaft mbH
Atos Spain S.A
Bulgarian Posts PLC
Croatian Academic and Research Network - CARNet and Croatian National CERT
Romanian National Computer Emergency Response Team - CERT-RO & Romanian Partners
Cognitive Security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

ACDC Team

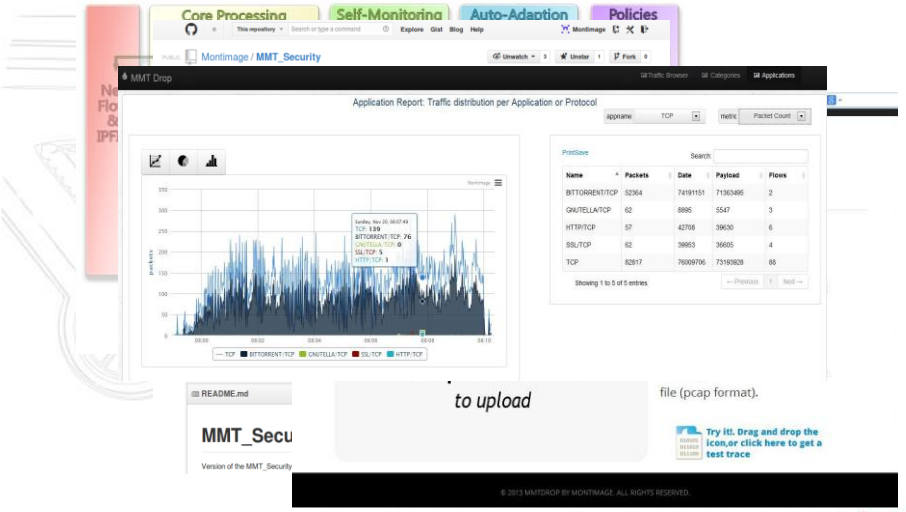
Fraunhofer FKIE
G Data Software AG
Institute for Internet Security, Gelsenkirchen University of Applied Sciences
INTECO - National Institute of Communication Technologies
KU Leuven
LSEC - Leaders in Security
Microsoft EMEA
SignalSpam
Telecom Italia
Telefonica I+D
University of Technology - Delft
XLAB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

21

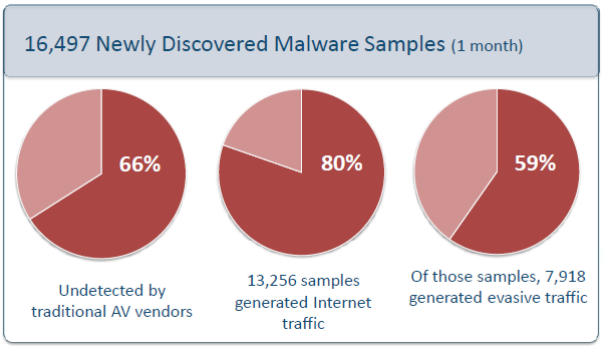
Consortium Structure



Component :Detect - Network Behaviour



Example



Preliminary ACDC Results - impact

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

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

Preliminary ACDC Results – impact

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

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

Preliminary ACDC Results – impact sharing

STIX™

Effective Cyber Threat Intelligence and Information Sharing

ACDC STIX Demonstrator

Query:

wordpress.com

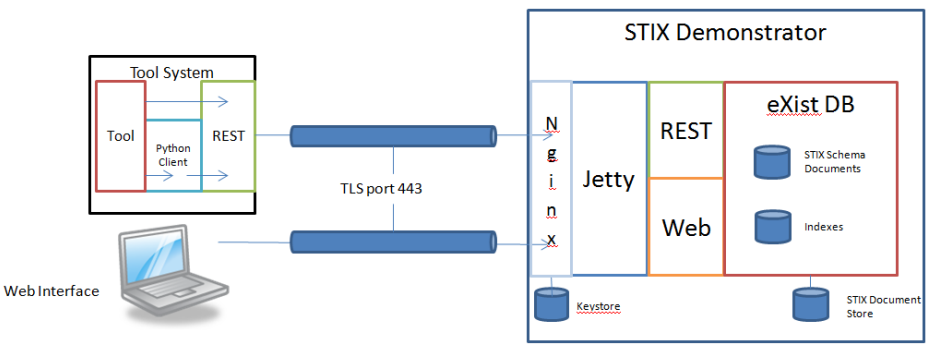
Query

Include testData?

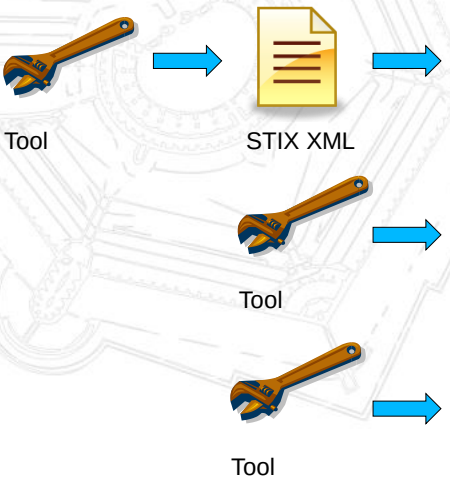
STIX_Package:ID	Created	stix:Title	Value
stix:package-cc5af045-8a4e-478d-b76b-783d6804054f	2013-09-19T14:02:01.337381	Malware URL with potential malware sample from CARNet Honeypot	http://buytwitterfollowerscheaply.wordpress.com/
stix:package-ee5ffd7d-c260-453a-9f7f-a5b5476caa5c	2013-09-19T14:01:48.882510	Malware URL with potential malware sample from CARNet Honeypot	http://www.martincrowe44.wordpress.com
stix:package-41d47941-0889-4f37-961f-6f4a8be3f316	2013-09-19T14:02:21.493909	Malware URL with potential malware sample from CARNet Honeypot	http://russiancasino.wordpress.com/

http://stix.mitre.org/

STIX Demonstrator Architecture



STIX Demonstrator via REST

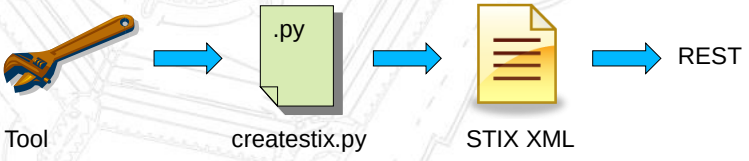


PUT method:
- Validates the XML against the STIX schema
- Stores the valid STIX document

DELETE method:
- Allows a tools to remove information that is no longer valid
- Can only delete "own" documents

Query method:
- Allows contents of the database to be searched based on STIX fragments
- GET method allows retrieval of full documents

STIX Demonstrator via CLI



Also deletestix.py to provided a CLI for deleting information.

Interface documentation and the python CLI available from the WP2 workspace.

Workshop : Sharing Exercise

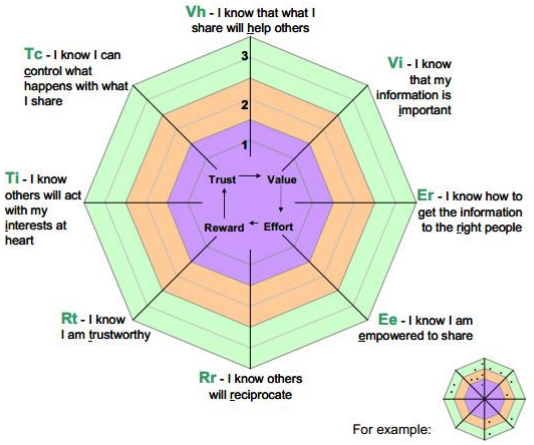
- self-awareness in relation to sharing sensitive information
- Sensitive : information which carries an element of risk to you as a person but could benefit another
- based on a model for sharing which came from some recent research conducted among a number of sharing forums in the UK

- assessment contains a number of statements, printed on cards
  - sort into two piles
  - from your viewpoint the statement is true they go on the TRUE pile
  - Other cards go on the FALSE pile
  - take no longer than 10 minutes to complete
  - at the end, you can analyse your results and see a visual representation

Workshop : Sharing Exercise

- Be able to make judgements :
  - Trust in the person with whom you are sharing;
  - Value of the information you are sharing;
  - Effort you need to expend to share;
  - Reward you would expect from sharing.

Workshop : Sharing Exercise



Assess yourself.

Information Sharing

- ISACs : Sector approach
  - Eg FS-ISAC, ISACs in NL
  - Trusted entities established by CI/KR owners and operators.
  - Comprehensive sector analysis
  - Reach-within their sectors, with other sectors, and with government to share critical information
  - All-hazards approach
  - Threat level determination for sector

ISACs

- Communications ISAC
- Electricity ISAC
- Emergency Management & Response ISAC
- Financial Services ISAC
- Highway ISAC
- Information Technology ISAC
- Maritime ISAC
- Multi-State ISAC

ISACs

- National Health ISAC
- Public Transit ISAC
- Real Estate ISAC
- Research and Education ISAC
- Supply Chain ISAC
- Surface Transportation ISAC
- Water ISAC

ISAC EXAMPLE: FS-ISAC Information Sharing and Analysis Tools for Members

- Cyber & Physical alerts from 24/7 Security Ops Center
- Briefings/white papers
- Risk Mitigation Toolkit
- Document Repository
- Anonymous Submissions
- Committee Listservs
- Member surveys
- Bi-weekly Threat calls
- Special info sharing member conference calls
- Crisis Management process– CMLT, CINS
- Semi-annual conferences
- Webinars
- Regional Program
- Viewpoints

Electricity ISAC

- The ES-ISAC's coverage includes bulk power system entities and 18 Reliability Coordinators and covers the entire continental United States and Canada
- Working on developing the necessary communication and participation with non-bulk power system entities and their critical suppliers
- www.esisac.com

Financial Services ISAC

- The only industry forum for collaboration on critical security threats facing the financial services sector
- Over 4,200 direct members and 30 member associations
- Ability to reach 99% of the banks and credit unions and 85% of the securities industry, and nearly 50% of the insurance industry
- www.fsisac.com

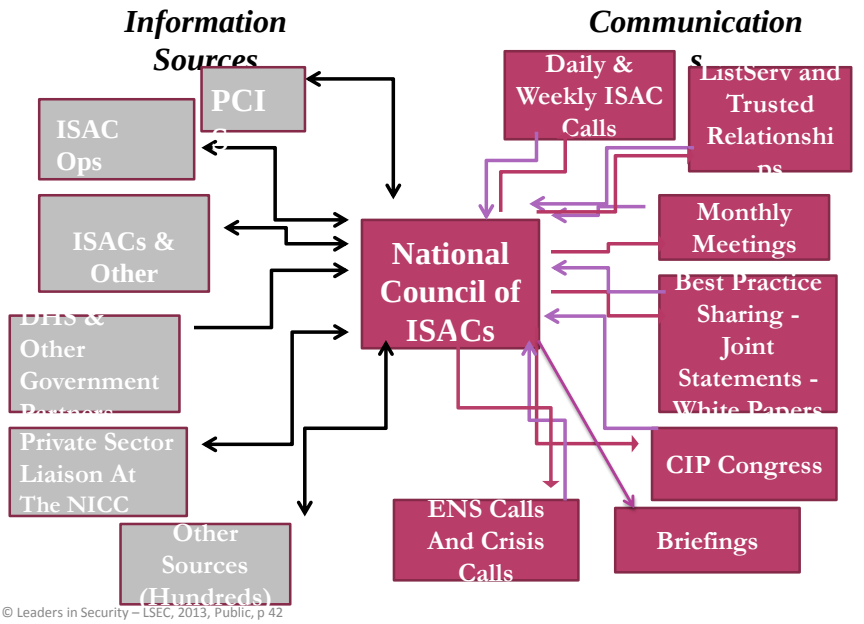
Information Technology ISAC

- Reaches 90% of all desktop operating systems, 85% of all databases; 76% of the global microprocessor market; 85% of all routers and 65% of software security

- www.it-isac.org

National Health ISAC

- The NH-ISAC serves to protect the nation's healthcare and public health critical infrastructure against security threats and vulnerabilities.
- Founded in 2010 leveraging Center for Technology Innovation at Kennedy Space Center
- Healthcare and Public Health organizations
- www.nhisac.org



DNS Cache Poisoning

When the DNS Cache Poisoning vulnerability was discovered in July 2008, ISACs alerted each other and shared mitigation strategies:

- Sector Call
- Information Sharing via ListServ
- Information Sharing via trusted relationships
- Weekly Inter-ISAC calls
- Joint Bulletin published by IT, Communications and FS ISACs

Support Center : botvrij.be

1. Under developments
2. Key Roles
   - first point of contact of victims suspecting cybercrime
   - resource of:
     - Information and knowledge for prevention
     - Awareness
     - Dissemination
   - Interact directly with end users – first level support
3. Tools:
   - Initiative-S: scan websites for possible infection
   - Botvrij.be: inform about botnets, clean infected computer clients, prevent future infections
   - ABBZ Anti Botnet Advisory Center : national support center consisting of a website and an user helpdesk with telephonic support
4. Business Service : sharing platform
5. Other services:
   - Support forum
   - Social network

NOT THE END

More information and follow-up

www.acdc-project.eu

This presentationandotherstuff (follow the BruCon link tomorrow) :

www.lsec.be

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