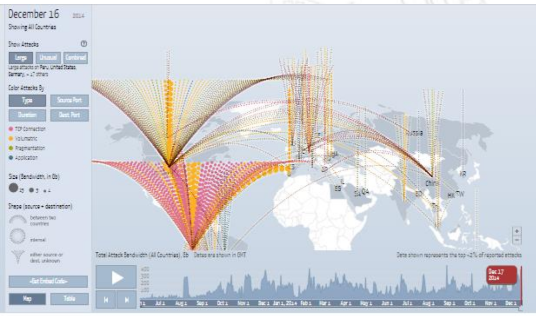
FIRST Conference – ISOC – CARIS Workshop

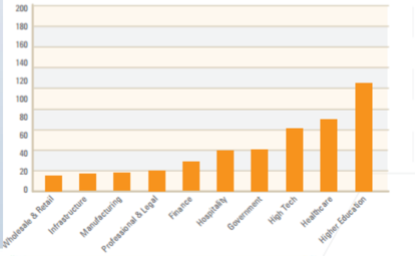
ACDC European Cyber Defence Pilot Experience

Ulrich Seldeslachts ,
Berlin, June 19th, 2015

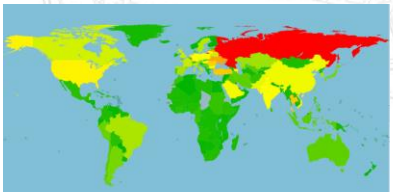
Constantly Under Attack



Avg Malicious Sessions / day per vertical



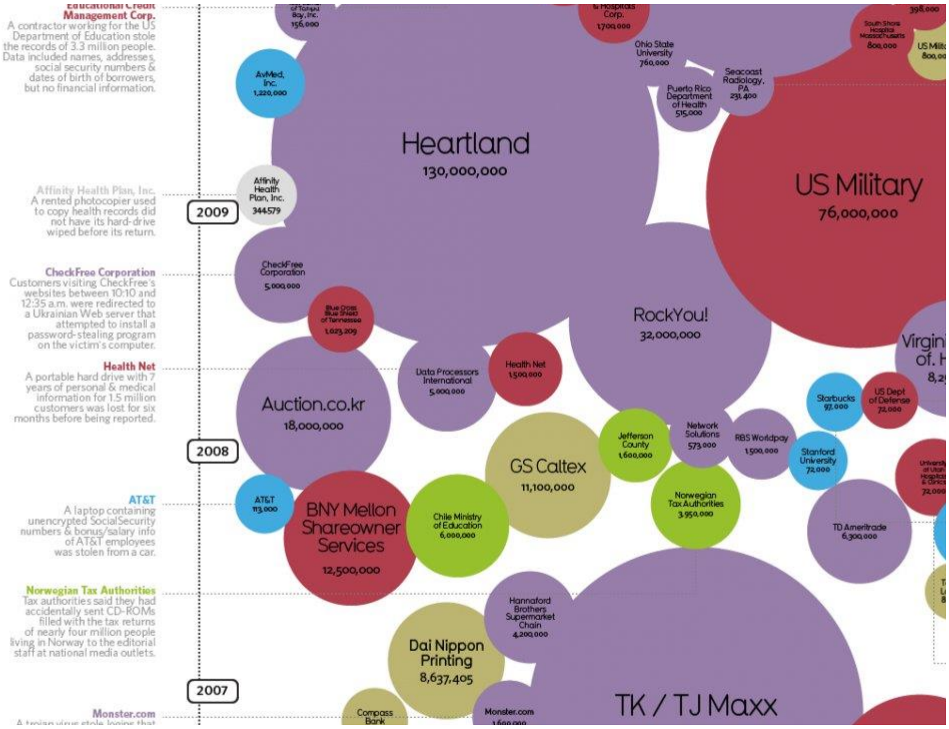
Sources : www.botvrij.be – digitalattackmap.com



Source : GlobalThreatMap Today

Minimum
Maximum

Source : Unit42, PA Wildfire, Threat Trend December 2014



Educational Credit Management Corp.
A contractor working for the US Department of Education stole the records of 3.3 million people. Data included names, addresses, social security numbers & dates of birth of borrowers, but no financial information.

Affinity Health Plan, Inc.
A rented photocopier used to copy health records did not have its hard-drive wiped before its return.

CheckFree Corporation
Customers visiting CheckFree's websites between 10:10 and 12:35 a.m. were redirected to a Ukrainian Web server that attempted to install a password-stealing program on the victim's computer.

Health Net
A portable hard drive with 7 years of personal & medical information for 1.5 million customers was lost for six months before being reported.

AT&T
A laptop containing unencrypted SocialSecurity numbers & bonus/salary info of AT&T employees was stolen from a car.

Norwegian Tax Authorities
Tax authorities said they had accidentally sent CD-ROMs filled with the tax returns of nearly four million people living in Norway to the editorial staff at national media outlets.

Monster.com

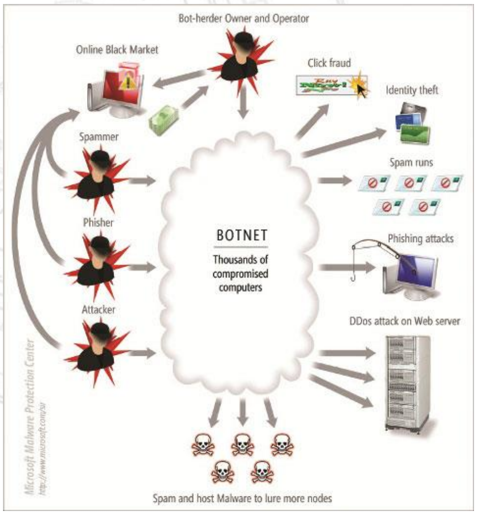
2009
2008
2007
of Tampa Bay, Inc. 156,000
AvMed, Inc. 1,220,000
Heartland 130,000,000
& Hospitals Corp. 1,700,000
Ohio State University 760,000
Puerto Rico Department of Health 515,000
Seacoast Radiology, PA 231,400
398,000
South Shore Hospital Massachusetts 800,000
US Milit 800,00
US Military 76,000,000
Affinity Health Plan, Inc. 344579
CheckFree Corporation 5,000,000
Blue Cross Blue Shield of Tennessee 1,023,209
RockYou! 32,000,000
Virgin of. H 8,2
Data Processors International 5,000,000
Health Net 1,500,000
Auction.co.kr 18,000,000
Starbucks 97,000
US Dept of Defense 72,000
GS Caltex 11,100,000
Jefferson County 1,600,000
Network Solutions 573,000
RBS Worldpay 1,500,000
Stanford University 72,000
University of Utah Hospitals & Clinics 72,000
AT&T 113,000
BNY Mellon Shareowner Services 12,500,000
Chile Ministry of Education 6,000,000
Norwegian Tax Authorities 3,950,000
TD Ameritrade 6,300,000
Hannaford Brothers Supermarket Chain 4,200,000
Dai Nippon Printing 8,637,405
Compass Bank
Monster.com 1,600,000
TK / TJ Maxx

Flow

1. Botnet Relevance?
2. SIEM Next Step : Information Sharing
3. ACDC : European Advanced Cyber Defense Center
4. About LSEC

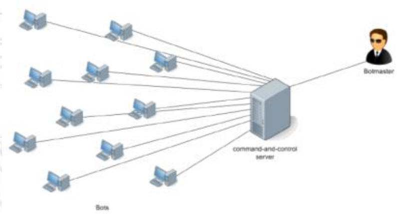
Botnets ?

What Botnets do

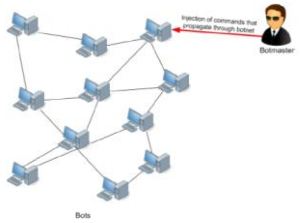

Bot-herder Owner and Operator
Online Black Market
Click fraud
Identity theft
Spammer
Spam runs
Phisher
BOTNET
Thousands of compromised computers
Phishing attacks
Attacker
DDos attack on Web server
Spam and host Malware to lure more nodes
Microsoft Malware Protection Center

Source : PCWorld

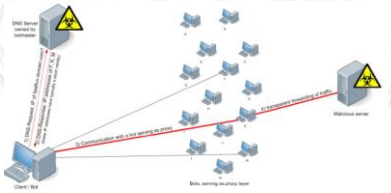
Botnet 1 : Centralised



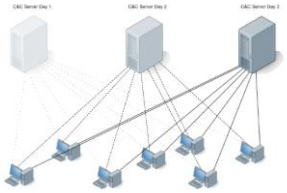
Botnet 2 : P2P



Botnet 3 : Fast Flux

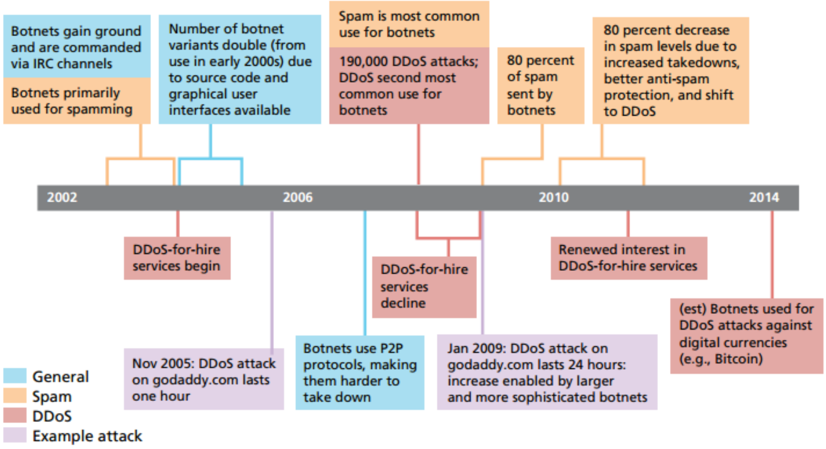

DNS Server owned by botmaster
1) DNS Request: IP of fastflux-domain.com?
2) DNS Response: IP addresses of F, K, M
3) Communication with a bot serving as proxy
4) transparent forwarding of traffic
Malicious server
Client / Bot
Bots, serving as proxy layer

Botnet 4 : Locomotive



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

Botnet History



Botnets gain ground and are commanded via IRC channels

Botnets primarily used for spamming

Number of botnet variants double (from use in early 2000s) due to source code and graphical user interfaces available

Spam is most common use for botnets

190,000 DDoS attacks; DDoS second most common use for botnets

80 percent of spam sent by botnets

80 percent decrease in spam levels due to increased takedowns, better anti-spam protection, and shift to DDoS

DDoS-for-hire services begin

DDoS-for-hire services decline

Renewed interest in DDoS-for-hire services

(est) Botnets used for DDoS attacks against digital currencies (e.g., Bitcoin)

Nov 2005: DDoS attack on godaddy.com lasts one hour

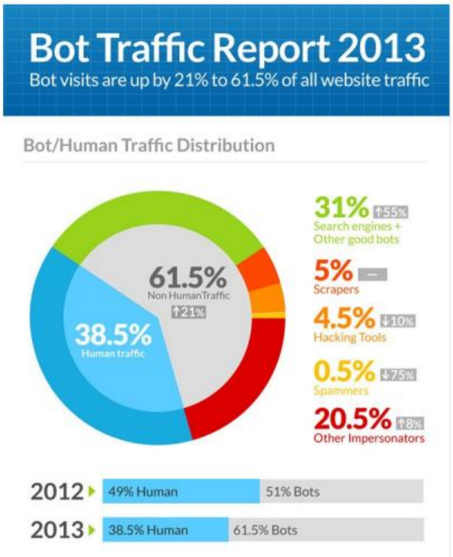
Botnets use P2P protocols, making them harder to take down

Jan 2009: DDoS attack on godaddy.com lasts 24 hours: increase enabled by larger and more sophisticated botnets

- 🟦 General
- 🟧 Spam
- 🟥 DDoS
- 🟪 Example attack

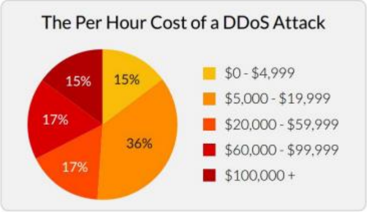
Source : RAND, Market for CyberCrime, 2014

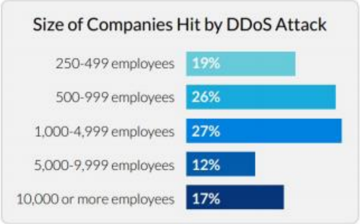
Bots?

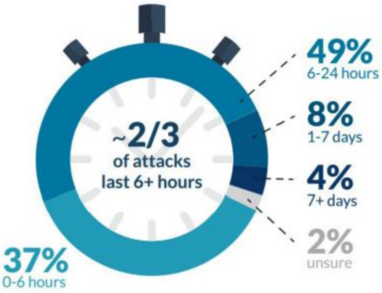


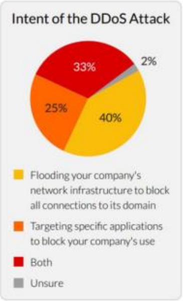
Source : RAND, Market for CyberCrime, 2014

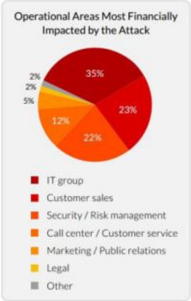
Botnets today ? DDoS









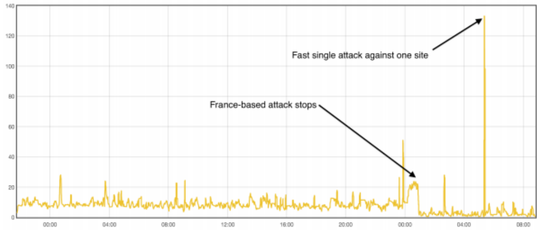


Source : Incapsula, Imperva, 11/2014

Botnets tomorrow : More Sophistication

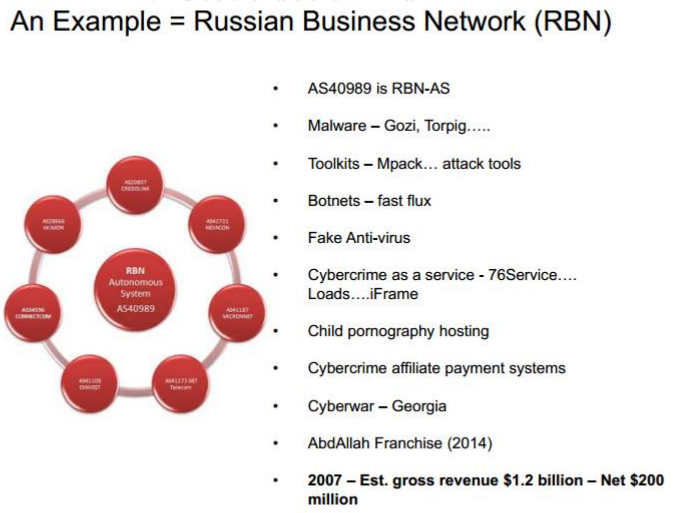
- Volumetric DDoS Attacks – brute force – with increasing amplification ?
- DNS Infrastructure Attacks? – dns resolver cache flood - taking down nameservers ?
- HTTP attacks – brute force against webservers ?
- Malicious Payloads – exploit server vulnerabilities – ShellShock

- Weaponize Attacks
- AWS Botnet ?
- New Large Botnets



Source : Cloudfare, December 2014 (Botconf)

Botnet is Big Business : Example RBN

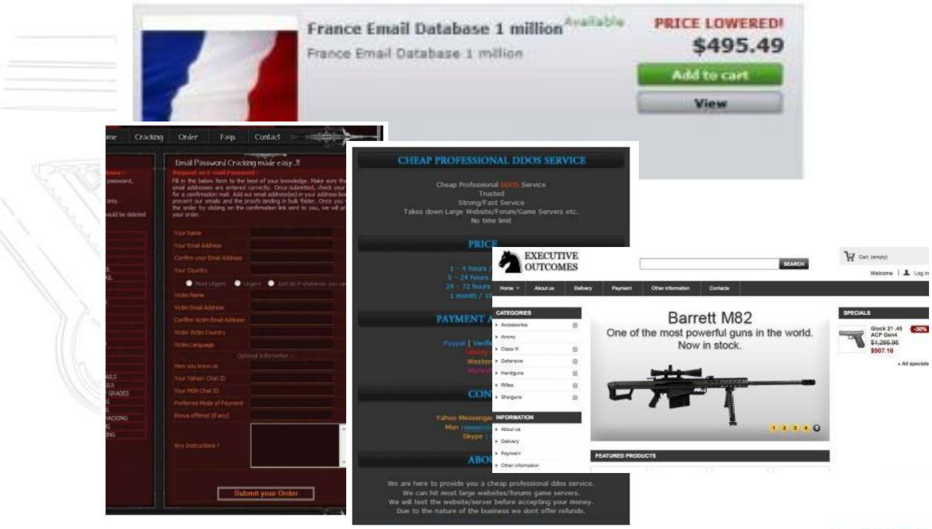

AS20807 CREDOLINK
AS41731 NEVACON
AS28866 AKIMON
RBN Autonomous System AS40989
AS34596 CONNECTCOM
AS41187 MICRONNET
AS41103 DINVEST
AS41173 SBT Telecom

An Example = Russian Business Network (RBN)

- AS40989 is RBN-AS
- Malware – Gozi, Torpig…..
- Toolkits – Mpack… attack tools
- Botnets – fast flux
- Fake Anti-virus
- Cybercrime as a service - 76Service…. Loads….iFrame
- Child pornography hosting
- Cybercrime affiliate payment systems
- Cyberwar – Georgia
- AbdAllah Franchise (2014)
- **2007 – Est. gross revenue $1.2 billion – Net $200 million**

Source : Cyberdefcon 03/2014 at LSEC, Infosecurity

Using webservices, Botnet as a Service, …



France Email Database 1 million Available

France Email Database 1 million

PRICE LOWERED!

$495.49

Add to cart

View

Cracking Order Faqs Contact

Email Password Cracking made easy..!!

Submit your Order

CHEAP PROFESSIONAL DDOS SERVICE

Cheap Professional DDOS Service
Trusted
Strong/Fast Service
Takes down Large Website/Forum/Game Servers etc.
No time limit

PRICE

PAYMENT

We are here to provide you a cheap professional ddos service.
We can hit most large websites/forums game servers.
We will test the website/server before accepting your money.
Due to the nature of the business we dont offer refunds.

EXECUTIVE OUTCOMES

CATEGORIES

INFORMATION

Barrett M82

One of the most powerful guns in the world. Now in stock.

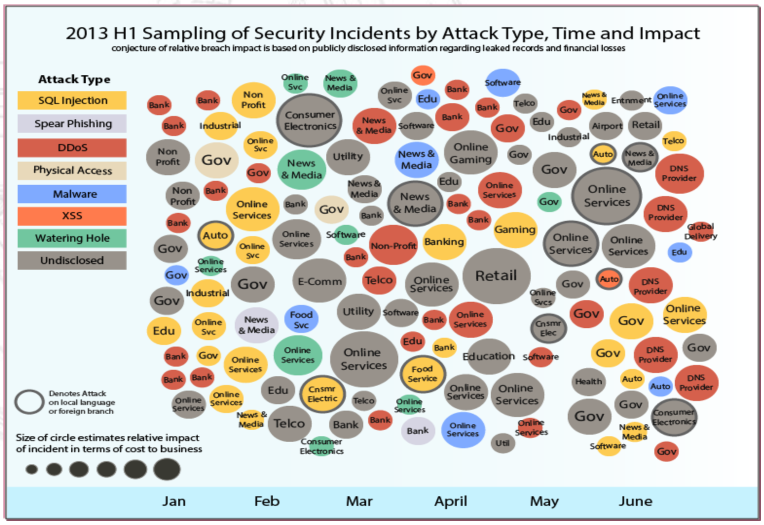
SPECIALS

FEATURED PRODUCTS

© Leaders in Security – LSEC, 2014, Public, p 13

Source : McAfee, Cybercrime Exposed, October 2013

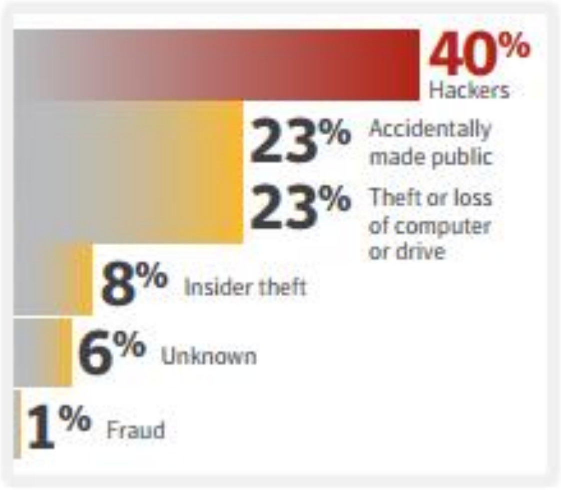
Doesn't impact your business?



© Leaders in Security – LSEC, 2014, Public, p 14

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

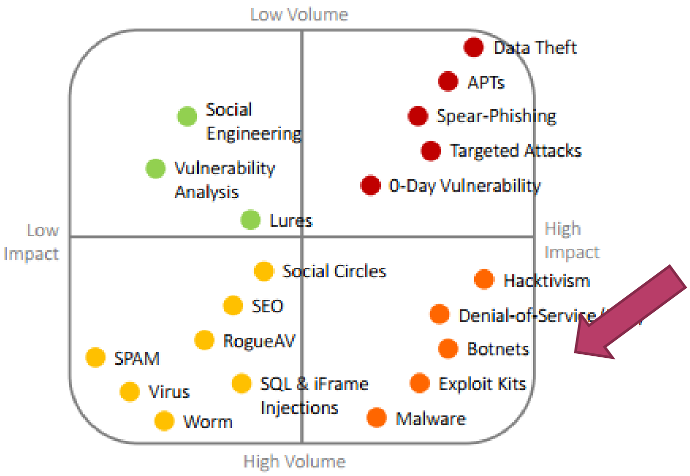
Attribution : top causes of data breaches 2012 - 13



© Leaders in Security – LSEC, 2014, Public, p 15

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

But who cares? – Business ? – not really



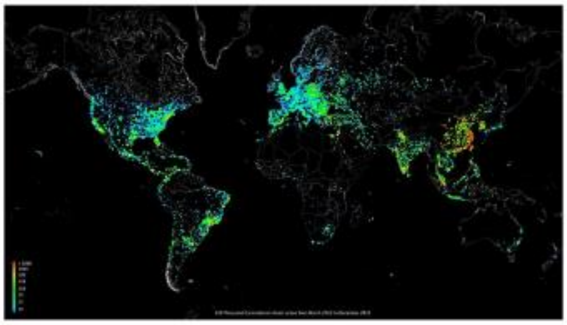
© Leaders in Security – LSEC, 2014, for ACDC – public , p 16

Source : LSEC, Innovations, Websense, 09/13

Should we even care?

Source : LSEC ACDC, Cyberdefcon March 2013

Carna Botnet : 420.000 bots – a research project

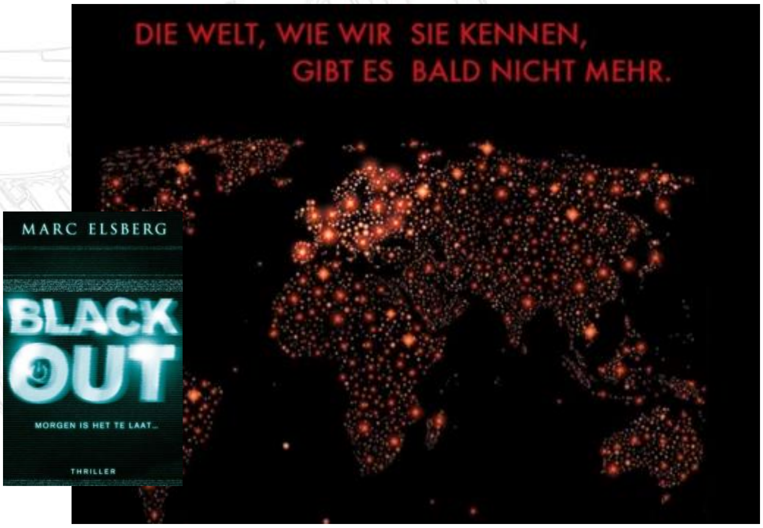


60k virus on an infected device:

- 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!

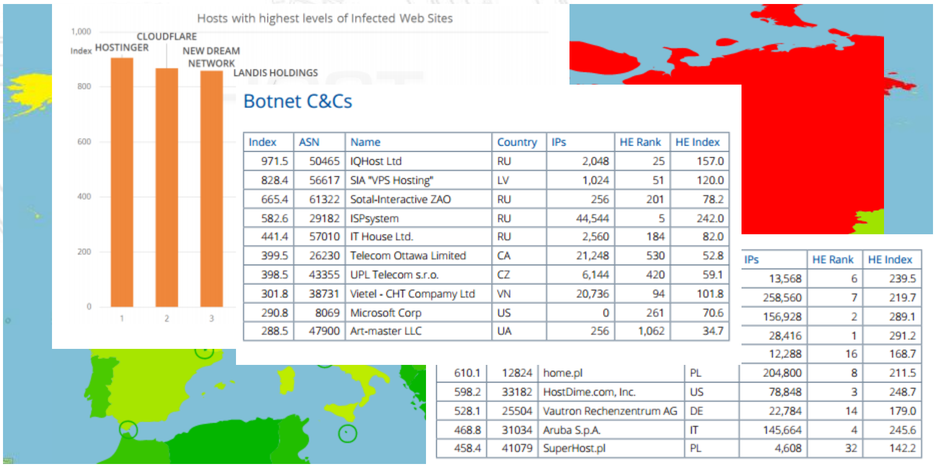
Source : LSEC, ACDC, Cyberdefcon 03/2013

The point?



Source : Marc Elsberg, Blackout, 2013

Global Threat Map Today



Botnet C&Cs

Index	ASN	Name	Country	IPs	HE Rank	HE Index
971.5	50465	IQHost Ltd	RU	2,048	25	157.0
828.4	56617	SIA "VPS Hosting"	LV	1,024	51	120.0
665.4	61322	Sotal-Interactive ZAO	RU	256	201	78.2
582.6	29182	ISPsystem	RU	44,544	5	242.0
441.4	57010	IT House Ltd.	RU	2,560	184	82.0
399.5	26230	Telecom Ottawa Limited	CA	21,248	530	52.8
398.5	43355	UPL Telecom s.r.o.	CZ	6,144	420	59.1
301.8	38731	Vietel - CHT Compamy Ltd	VN	20,736	94	101.8
290.8	8069	Microsoft Corp	US	0	261	70.6
288.5	47900	Art-master LLC	UA	256	1,062	34.7

				IPs	HE Rank	HE Index
				13,568	6	239.5
				258,560	7	219.7
				156,928	2	289.1
				28,416	1	291.2
				12,288	16	168.7
610.1	12824	home.pl	PL	204,800	8	211.5
598.2	33182	HostDime.com, Inc.	US	78,848	3	248.7
528.1	25504	Vautron Rechenzentrum AG	DE	22,784	14	179.0
468.8	31034	Aruba S.p.A.	IT	145,664	4	245.6
458.4	41079	SuperHost.pl	PL	4,608	32	142.2

Source : Hostexploit, March 2014

Botnet Relevance for Business

Source : various, GoDaddy, Checkpoint

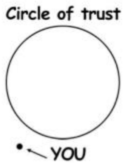
Why Information Sharing?

Business Case components for trusted sharing

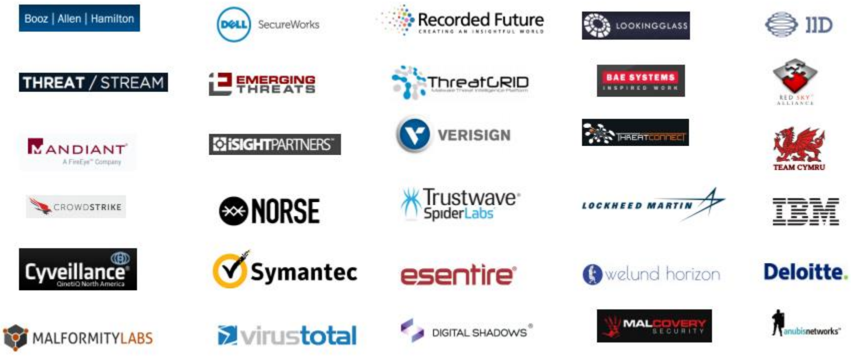
Forrester defines threat intelligence as:

Source : Forrester Research, 2014

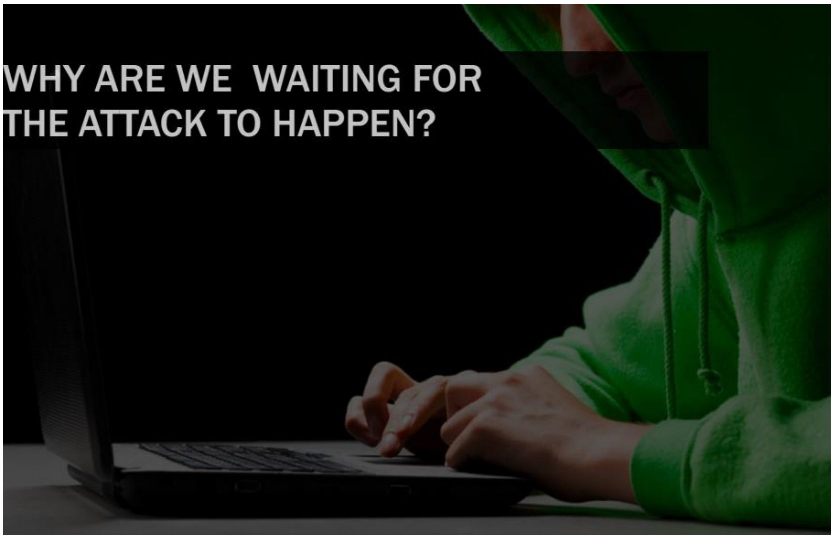
- Details of the motivations, intent, and capabilities of internal and external threat actors. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. *Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats.*
- We share at about the same speed that George R.R. Martin writes novels, which is slow
- Quid pro quo and relationship driven
- You cannot automate trust



Not alone … need to differentiate



The need for Active Defense



Source : RSA Conference, OpenDNS, 02/14

The Threat landscape

Web-based malicious activity has accelerated

- Primary vector for malicious activity
- Target reputable, high-traffic websites

Cyber criminals want YOUR information

- Focus on exploits targeting end-users for financial gain

Increased sophistication of the Underground Economy

- Well-established infrastructure for monetizing stolen information

Rapid adaptation to security measures

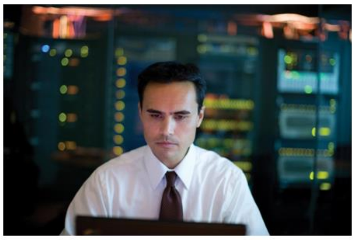
- Relocating operations to new geographic areas
- Evade traditional security protection

Source : Symantec, Deepsight EWS, 2012

Threat landscape

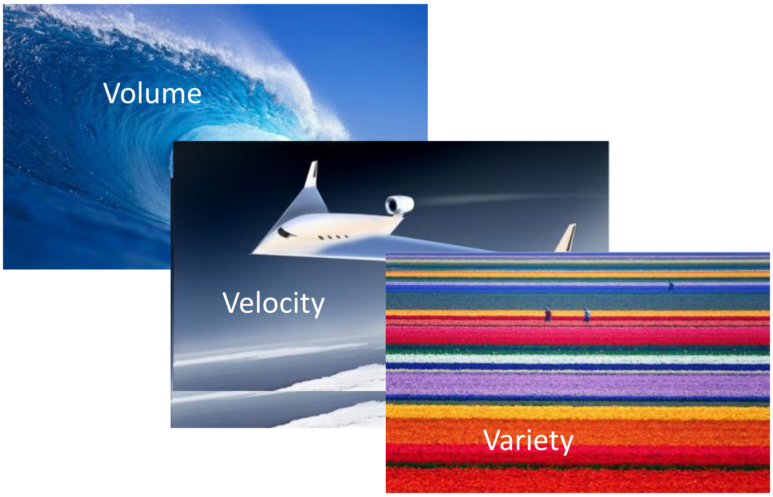
The Challenge

- How do I gain awareness of the global threat landscape?
- How do I identify threats that could impact my company?
  - 31,850 new malicious code threats per week*
- How do I identify vulnerabilities important to my company?
  - 105 new vulnerabilities per week *
- How do I prioritize my response to vulnerabilities and global threats?
- How do I translate the global landscape to my enterprise?

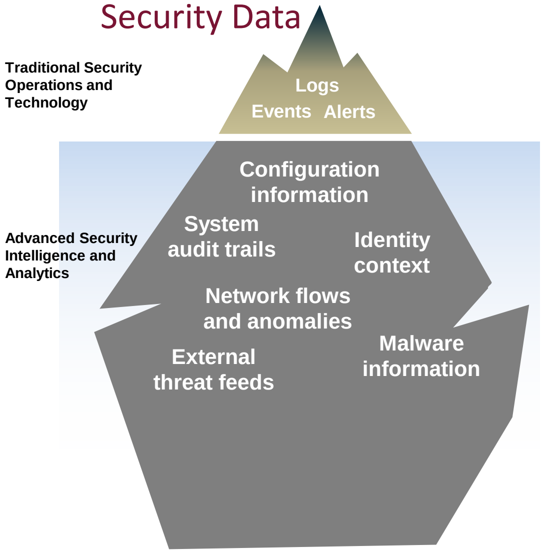


Source : Symantec, Deepsight EWS, 2012

Threats are BIG



The Methodology : 1 Collect and Store Security Data


Traditional Security Operations and Technology
Logs
Events Alerts
Advanced Security Intelligence and Analytics
Configuration information
System audit trails
Identity context
Network flows and anomalies
Malware information
External threat feeds

People

Data

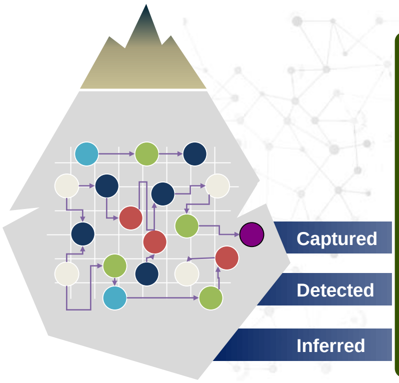
Applications

Infrastructure

Monitor Everything

Source : LSEC Big Data, IBM 0/14

The Methodology : 2 Real-time and historical analysis



Descriptive Analytics

- What happened?
- How many, how often, where?
- What exactly is the problem?
- What is the impact?

Historic and Predictive Analytics

- Has it happened before?
- What if these trends continue?
- What might happen next?

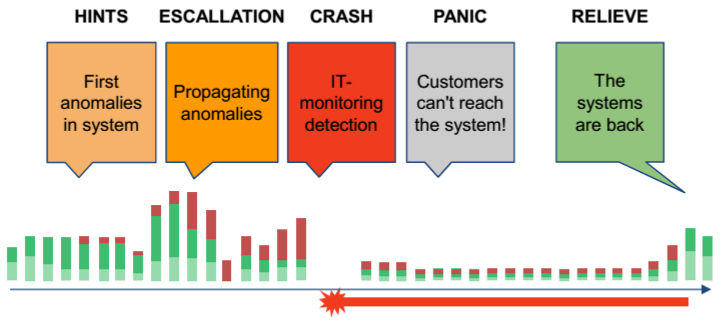
Decision modeling

- What actions can we take?
- How can we avoid this in future?
- How can we mitigate risk?

Data — Information → Security Intelligence

Source : LSEC Big Data, IBM 0/14

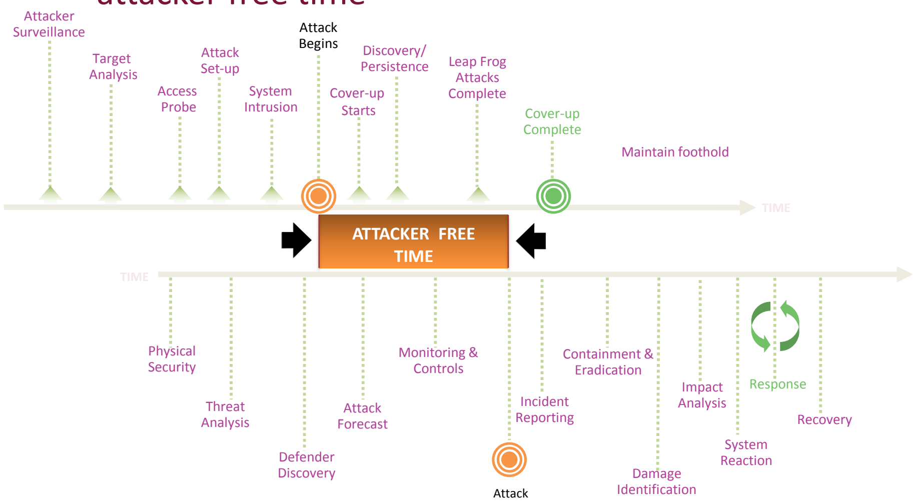
Operations Incident Handling



In reality, 25 hour incident
… and 11 hours before the effect

Source : LSEC Hardening, CrossRoad 03/14

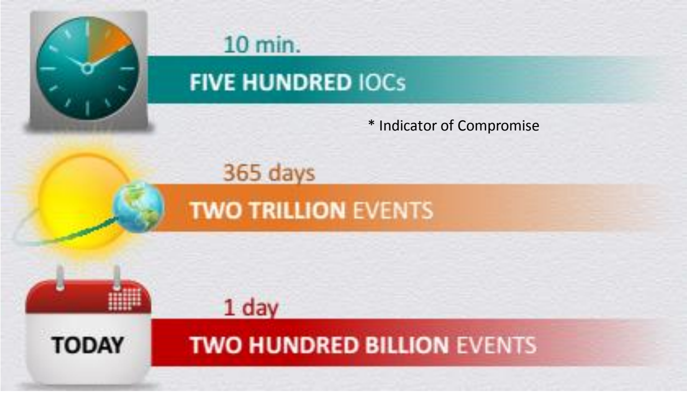
Operations Incident Handling : reducing attacker free time



Source: NERC HILF Report, June 2010 (http://www.nerc.com/files/HILF.pdf)

Source : LSEC Big Data, RSA, 01/13

Big Data in Security Events



10 min.
FIVE HUNDRED IOCs

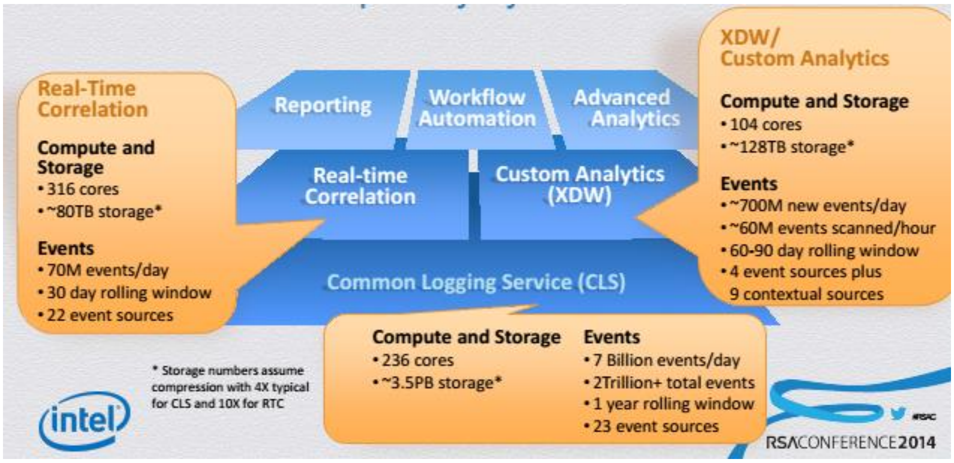
* Indicator of Compromise

365 days
TWO TRILLION EVENTS

1 day
TWO HUNDRED BILLION EVENTS

Source : RSA Conference, Intel 03/14

Analysis of incidents and threats



Real-Time Correlation

Compute and Storage
- 316 cores
- ~80TB storage*

Events
- 70M events/day
- 30 day rolling window
- 22 event sources

XDW/ Custom Analytics

Compute and Storage
- 104 cores
- ~128TB storage*

Events
- ~700M new events/day
- ~60M events scanned/hour
- 60-90 day rolling window
- 4 event sources plus 9 contextual sources

Compute and Storage
- 236 cores
- ~3.5PB storage*

Events
- 7 Billion events/day
- 2Trillion+ total events
- 1 year rolling window
- 23 event sources

* Storage numbers assume compression with 4X typical for CLS and 10X for RTC

Source : RSA Conference, Intel 03/14

Breach Notification – required / voluntary

ACDC the Advanced Cyber Defence Centre

EUROPEAN COMMISSION

Brussels, 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

concerning measures to ensure a high common level of network and information security across the Union

{SWD(2013) 31 final}
{SWD(2013) 32 final}

CHAPTER IV

SECURITY OF THE NETWORKS AND INFORMATION SYSTEMS OF PUBLIC ADMINISTRATIONS AND MARKET OPERATORS

Article 14

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

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

http://www.networkworld.com/news/2013/091213-hack victims-273795.html?page=2

Press release

Government launches information sharing partnership on cyber security

Organisation:	Cabinet Office
Page history:	Published 27 March 2013
Policy:	Keeping the UK safe in cyber space
Topic:	National security
Minister:	The Rt Hon Francis Maude MP

CiSP
A CATALYST FOR COLLABORATION

New cyber partnership launched to help government and industry share information and intelligence on cyber security threats.

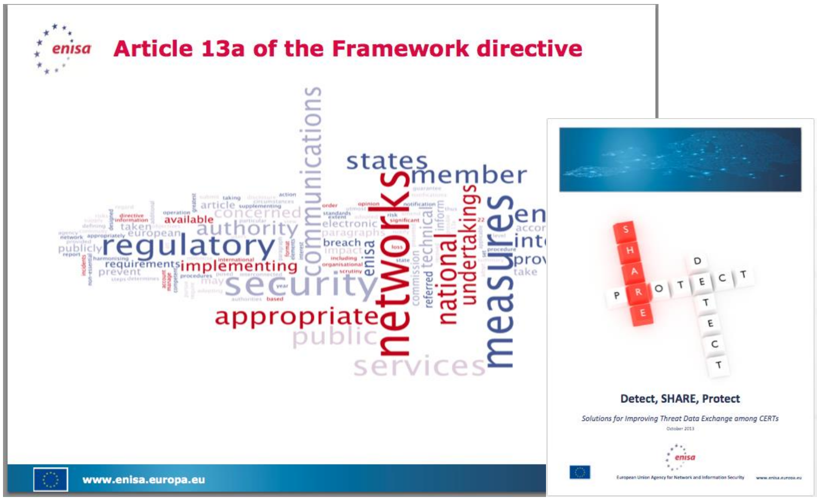
https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security

Sharing
the Wealth,
and the
Burdens,
of Threat
Intelligence

WARP
Warning, advice
and reporting point

Example Regulatory : Telecom

ACDC the Advanced Cyber Defence Centre


enisa **Article 13a of the Framework directive**

Detect, SHARE, Protect

Solutions for Improving Threat Data Exchange among CERTs

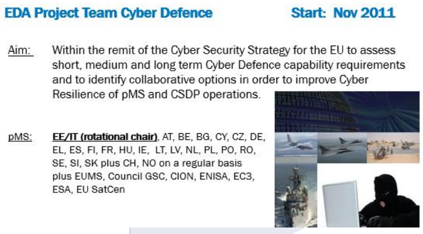
October 2013

enisa

European Union Agency for Network and Information Security www.enisa.europa.eu

Those looking to multiply their knowledge, should be prepared to share some first

Example Voluntary – Information Sharing



EDA Project Team Cyber Defence **Start: Nov 2011**

Aim: Within the remit of the Cyber Security Strategy for the EU to assess short, medium and long term Cyber Defence capability requirements and to identify collaborative options in order to improve Cyber Resilience of pMS and CSDP operations.

pMS: EE/IT (rotational chair), AT, BE, BG, CY, CZ, DE, EL, ES, FI, FR, HU, IE, LT, LV, NL, PL, PO, RO, SE, SI, SK plus CH, NO on a regular basis plus EUMS, Council GSC, CION, ENISA, EC3, ESA, EU SatCen

EUROPEAN DEFENCE AGENCY

ACDC

IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

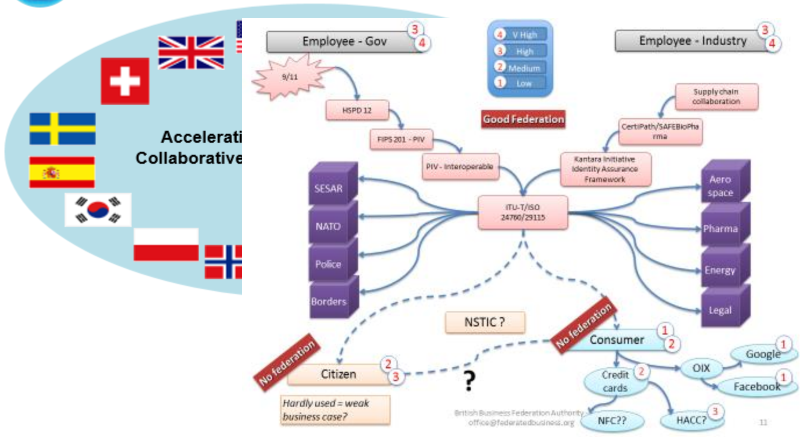
NCI AGENCY
NATO Communications and Information Agency

FIRST
Improving Security Together

Cyber Security Data Exchange and Collaboration Infrastructure (CDXI)

Example Voluntary – Information Sharing

Multinational Alliance for Collaborative Cyber Situational Awareness



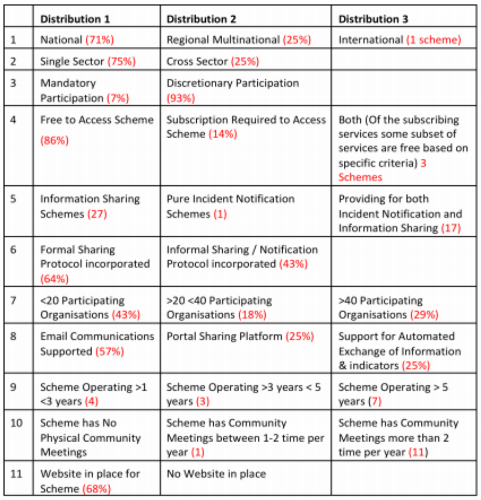
Source : LSEC – NCSC, InfoSharing, MACSSA, 2014

Club R2GS

© Leaders in Security – LSEC, 2014, Public – Closed User Group Distribution, p 39

Information Sharing : NISP Survey Results

Summary of 32 Scheme Responses



	Distribution 1	Distribution 2	Distribution 3
1	National (71%)	Regional Multinational (25%)	International (1 scheme)
2	Single Sector (75%)	Cross Sector (25%)	
3	Mandatory Participation (7%)	Discretionary Participation (93%)	
4	Free to Access Scheme (86%)	Subscription Required to Access Scheme (14%)	Both (Of the subscribing services some subset of services are free based on specific criteria) 3 Schemes
5	Information Sharing Schemes (27)	Pure Incident Notification Schemes (1)	Providing for both Incident Notification and Information Sharing (17)
6	Formal Sharing Protocol incorporated (64%)	Informal Sharing / Notification Protocol incorporated (43%)	
7	<20 Participating Organisations (43%)	>20 <40 Participating Organisations (18%)	>40 Participating Organisations (29%)
8	Email Communications Supported (57%)	Portal Sharing Platform (25%)	Support for Automated Exchange of Information & indicators (25%)
9	Scheme Operating >1 <3 years (4)	Scheme Operating >3 years < 5 years (3)	Scheme Operating > 5 years (7)
10	Scheme has No Physical Community Meetings	Scheme has Community Meetings between 1-2 time per year (1)	Scheme has Community Meetings more than 2 time per year (11)
11	Website in place for Scheme (68%)	No Website in place	

© Leaders in Security – LSEC, 2014, for ACDC – public , p 40

Source : NISP, WG2, 3rd plenary, 04.14

Club R2GS

Howto : Incident Management Tools

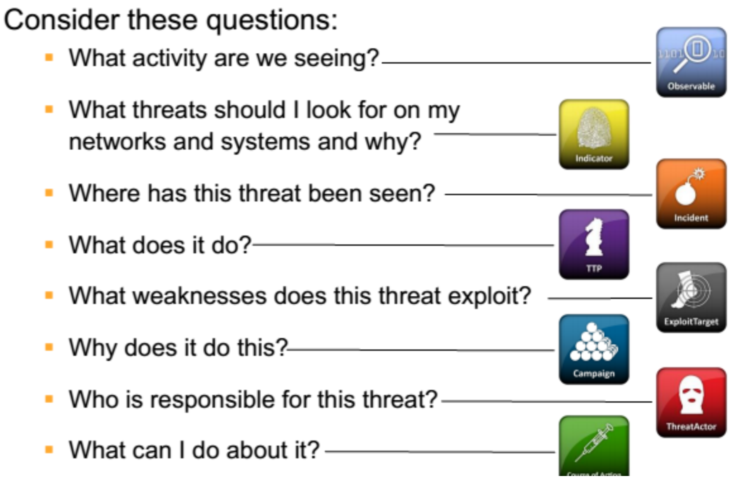
STIX™

Effective Cyber Threat Intelligence and Information Sharing

http://stix.mitre.org/

Information Sharing : commonalities, no conflict

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/

US DHS – FIRST – ADCC – LSEC July 2014

Representatives of NATO, industry, end users, CERTs, …

Club R2GS

ACDC

Advanced Cyber Defence Center

Club R2GS

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 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.

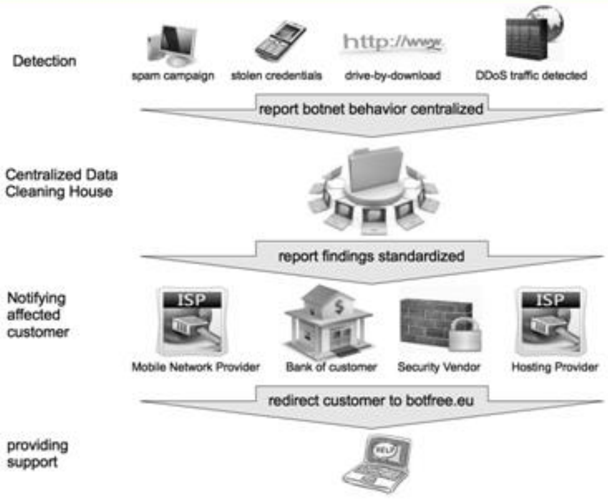
Fundació Privada Barcelona Digital Centre Tecnològic

Istituto Superiore Delle Comunicazioni e delle Tecnologie dell'Informazione

Montimage

ACDC

Solution



ACDC the Advanced Cyber Defence Centre

AC up to today – DC

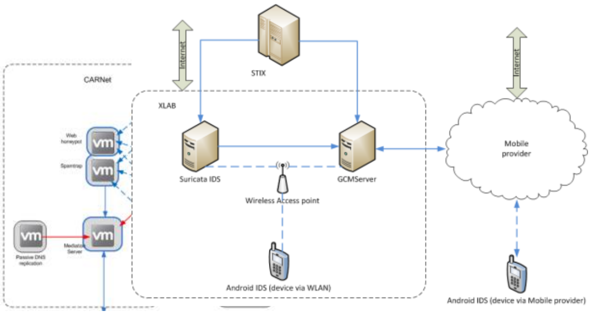
1. Achievement Highlights
   1. Collaboration 28 partners, 14 countries, +40 external partners
   2. Sensors operational, sensing, analyzing, reporting locally & sending data to Central Clearing House (CCH)
   3. New sensors installed & operational (eg Darknet)
   4. CCH operational and collecting and transmitting data (JSON, YAML), STIX integration
   5. Decentralized Data Analysis with 6 different industrial partners
   6. Reporting into CERTs, ISP’s, LEA’s … end users
   7. Setup of 11 National Support Centers
   8. Different resulting tools : Mobile, Ransomware, Website Check, …

2. Challenges Highlights
   1. Regulatory Framework : Data Protection vs Monitoring
      1. Consent
      2. Controlled :
         1. ISPs – CERTs by exception
         2. Industry – delegated
   2. Performance & Capability of Detection & Takedown
   3. Sustainability of the Community : sign up today!

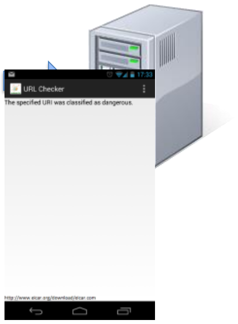
5
EXPERIMENTS
8
SUPPORT CENTERS
1 Data Clearing House

Data Sharing : Example & Effect

CARNet creates identified threat information and sends the information to ACDC



CCH



The specified URI was classified as dangerous.

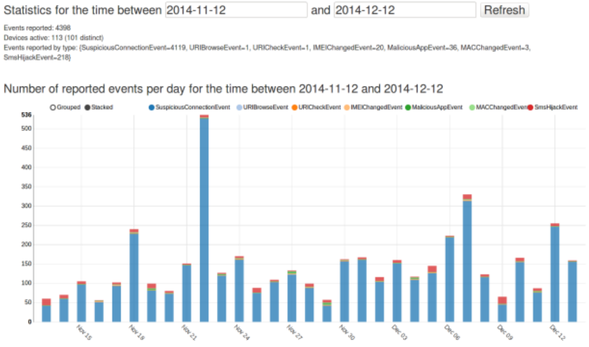
http://www.eicar.org/download/eicar.com

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

XLAB Mobile IDS : Device Monitor

- 33 Android botnets
  - 1-co Symbian botnet with the same C&C!
- 2 Symbian botnets
- 3 Blackberry botnets
- Statistics from 10/8/2014, 14.077 infections total

Source : K&A Virus Tracker, Botconf 2014



Statistics for the time between 2014-11-12 and 2014-12-12 Refresh

Events reported: 4398
Devices active: 113 (101 distinct)
Events reported by type: {SuspiciousConnectionEvent=4119, URIBrowseEvent=1, URICheckEvent=1, IMEIChangedEvent=20, MaliciousAppEvent=36, MACChangedEvent=3, SmsHijackEvent=218}

Number of reported events per day for the time between 2014-11-12 and 2014-12-12

Source : ACDC Internal, XLAB, 2014

Available on Google Play Store

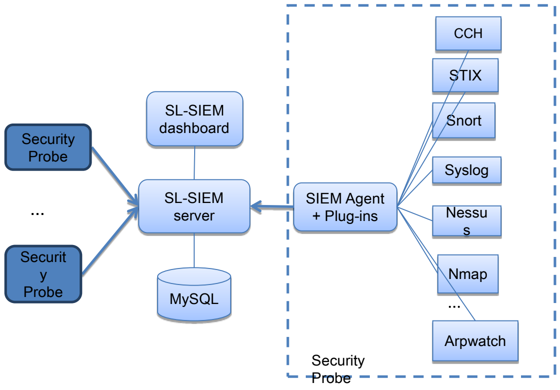
- https://play.google.com/store/apps/details?id=eu.acdc.xlab.devicemonitor
- Demo videos: http://x.k00.fr/zmprk

Get it on Google play

Tools in Production to Solutions

ACDC the Advanced Cyber Defence Centre

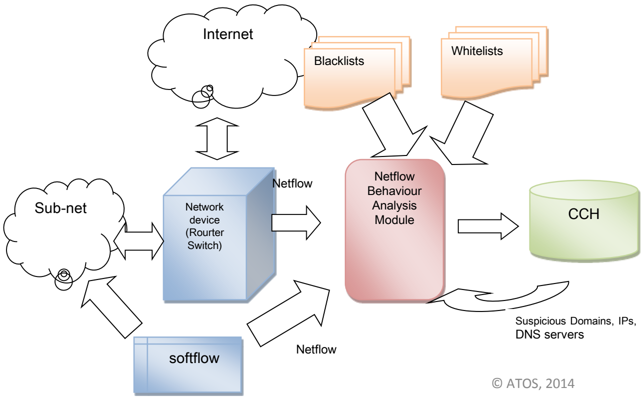
ATOS AHPS, commercial SIEM



© ATOS, 2014

Tools in Production to Solutions

ATOS Netflow Behavorial Analysis


Internet
Blacklists
Whitelists
Sub-net
Network device (Rourter Switch)
Netflow
Netflow Behaviour Analysis Module
CCH
Suspicious Domains, IPs, DNS servers
softflow
Netflow

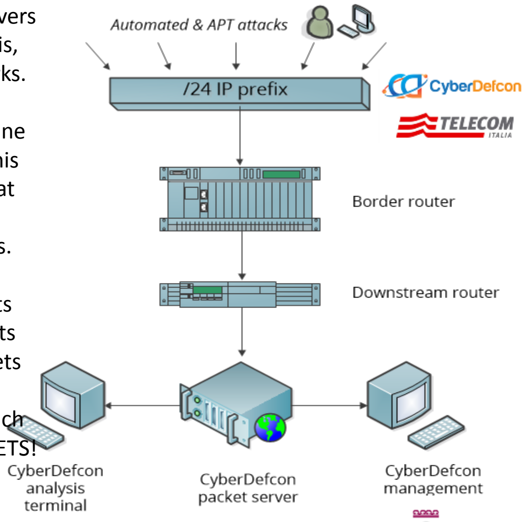
© ATOS, 2014

Darknet Subpilot

A Darknet is a portion of routed, allocated IP space in which no active services or servers reside. These are "dark" because there is, seemingly, nothing within these networks.

A Darknet does in fact include at least one server, designed as a packet vacuum. This server gathers the packets and flows that enter the Darknet, useful for real-time analysis or post-event network forensics.

Any packet that enters a Darknet is by its presence aberrant. No legitimate packets should be sent to a Darknet. Such packets may have arrived by mistake or misconfiguration, but the majority of such packets are sent by malware and BOTNETS!

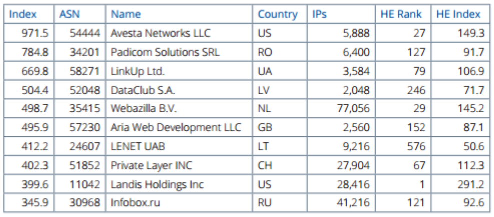


Darknet Subpilot

- Darknet Results : Most Seen ASN's

ASN	Name	Country	Subnet sizes	Requests	Request ratio	HE Rank	HE Index
16276	OVH	FR	1,090,816	124,059	0.114	12	182.24
4134	CHINANET	CN	104,621,312	55,003	0.001	46	124.88
6939	HURRICANE	US	260,864	37,095	0.142	393	60.49
29073	ECATEL	NL	9,984	31,850	3.190	19	162.89
36352	COLOCROSSING	US	122,368	25,898	0.212	230	74.23
12876	ONLINE S.A.S.	FR	180,224	24,290	0.135	1,371	29.02
4837	CHINA169	CN	53,008,896	23,811	0.000	48	122.68
3462	HINET	TW	8,085,504	13,983	0.002	123	92.50
45090	CNNIC-TENCENT	CN	6,656	13,873	2.084	45,553	0.19
4766	KIXS-AS	KR	29,005,312	12,895	0.000	262	70.58

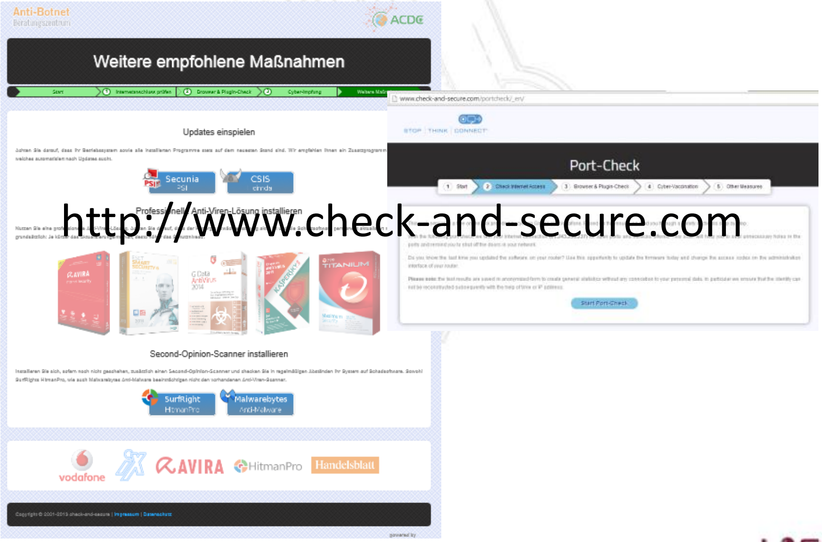
- Providing Input into : Hostexploits Report on Zeus Botnet



Index	ASN	Name	Country	IPs	HE Rank	HE Index
971.5	54444	Avesta Networks LLC	US	5,888	27	149.3
784.8	34201	Padicom Solutions SRL	RO	6,400	127	91.7
669.8	58271	LinkUp Ltd.	UA	3,584	79	106.9
504.4	52048	DataClub S.A.	LV	2,048	246	71.7
498.7	35415	Webazilla B.V.	NL	77,056	29	145.2
495.9	57230	Aria Web Development LLC	GB	2,560	152	87.1
412.2	24607	LENET UAB	LT	9,216	576	50.6
402.3	51852	Private Layer INC	CH	27,904	67	112.3
399.6	11042	Landis Holdings Inc	US	28,416	1	291.2
345.9	30968	Infobox.ru	RU	41,216	121	92.6

Source : http://hostexploit.com/, March 2014

User Tools & impact



Anti-Botnet
Beratungszentrum

Weitere empfohlene Maßnahmen

Updates einspielen

Achten Sie darauf, dass Ihr Betriebssystem sowie alle installierten Programme stets auf dem neuesten Stand sind. Wir empfehlen Ihnen ein Zusatzprogramm, welches automatisch nach Updates sucht.

Professionelle Anti-Viren-Lösung installieren

Nutzen Sie eine professionelle Anti-Viren-Lösung. Achten Sie darauf, dass der [illegible] alle [illegible] Schutzsoftware permanent aktualisiert [illegible] grundsätzlich: Je kürzer das Aktualisierungsintervall, desto höher das Schutzniveau.

Second-Opinion-Scanner installieren

Installieren Sie sich, sofern noch nicht geschehen, zusätzlich einen Second-Opinion-Scanner und checken Sie in regelmäßigen Abständen Ihr System auf Schadsoftware. Sowohl SurfRights HitmanPro, wie auch Malwarebytes Anti-Malware beeinträchtigen nicht den vorhandenen Anti-Viren-Scanner.

Copyright © 2001-2013 check-and-secure | Impressum | Datenschutz

powered by

www.check-and-secure.com/portcheck/_en/

Port-Check

[illegible]

With the following port check, we test your Internet connection ([illegible]) for open ports and services offered. This scan will help you to seal unnecessary holes in the ports and remind you to shut off the doors in your network.

Do you know the last time you updated the software on your router? Use this opportunity to update the firmware today and change the access codes on the administration interface of your router.

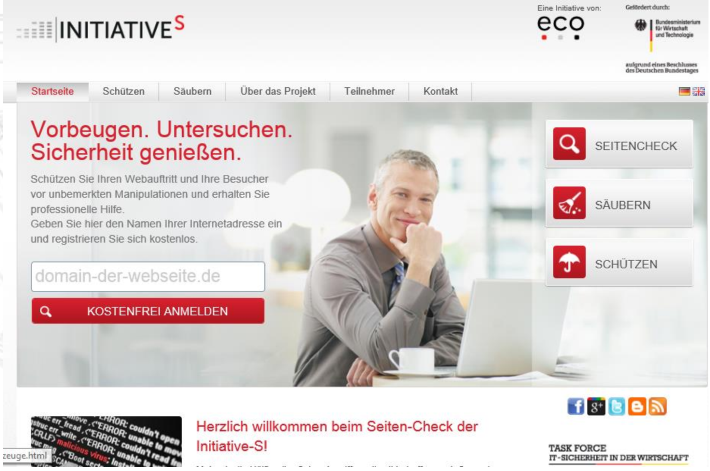
Please note: the test results are saved in anonymized form to create general statistics without any connection to your personal data. In particular we ensure that the identity can not be reconstructed subsequently with the help of time or IP address.

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



INITIATIVE S
Eine Initiative von: eco
Gefördert durch: Bundesministerium für Wirtschaft und Technologie
aufgrund eines Beschlusses des Deutschen Bundestages
Startseite
Schützen
Säubern
Über das Projekt
Teilnehmer
Kontakt
SEITENCHECK
SÄUBERN
SCHÜTZEN
KOSTENFREI ANMELDEN
TASK FORCE IT-SICHERHEIT IN DER WIRTSCHAFT

Vorbeugen. Untersuchen. Sicherheit genießen.

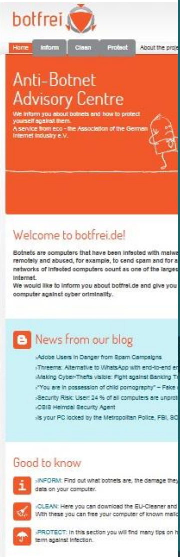
Schützen Sie Ihren Webauftritt und Ihre Besucher vor unbemerkten Manipulationen und erhalten Sie professionelle Hilfe.
Geben Sie hier den Namen Ihrer Internetadresse ein und registrieren Sie sich kostenlos.

domain-der-webseite.de

Herzlich willkommen beim Seiten-Check der Initiative-S!

zeuge.html

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



Anti-Botnet Advisory Centre

We inform you about botnets and how to protect yourself against them.
A service from eco - the Association of the German Internet Industry e.V.

Welcome to botfrei.de!

Botnets are computers that have been infected with malwa remotely and abused, for example, to send spam and for a networks of infected computers count as one of the large internet.
We would like to inform you about botfrei.de and give you computer against cyber criminality.

News from our blog

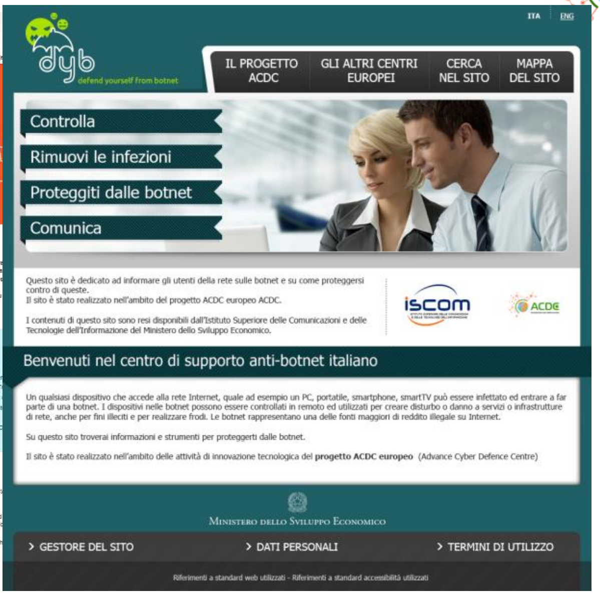
›Adobe Users in Danger from Spam Campaigns
›Threema: Alternative to WhatsApp with end-to-end e
›Making Cyber-Thefts visible: Fight against Banking T
›"You are in possession of child pornography" – Fake
›Security Risk: User! 24 % of all computers are unprot
›CSIS Heimdal Security Agent
›Is your PC locked by the Metropolitan Police, FBI, SC

Good to know

›INFORM: Find out what botnets are, the damage they data on your computer.

›CLEAN: Here you can download the EU-Cleaner and With these you can free your computer of known malic

›PROTECT: In this section you will find many tips on h term against infection.



Questo sito è dedicato ad informare gli utenti della rete sulle botnet e su come proteggersi contro di queste.
Il sito è stato realizzato nell'ambito del progetto ACDC europeo ACDC.

I contenuti di questo sito sono resi disponibili dall'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione del Ministero dello Sviluppo Economico.

Benvenuti nel centro di supporto anti-botnet italiano

Un qualsiasi dispositivo che accede alla rete Internet, quale ad esempio un PC, portatile, smartphone, smartTV può essere infettato ed entrare a far parte di una botnet. I dispositivi nelle botnet possono essere controllati in remoto ed utilizzati per creare disturbo o danno a servizi o infrastrutture di rete, anche per fini illeciti e per realizzare frodi. Le botnet rappresentano una delle fonti maggiori di reddito illegale su Internet.

Su questo sito troverai informazioni e strumenti per proteggerti dalle botnet.

Il sito è stato realizzato nell'ambito delle attività di innovazione tecnologica del **progetto ACDC europeo** (Advance Cyber Defence Centre)

Riferimenti a standard web utilizzati - Riferimenti a standard accessibilità utilizzati

www.botvrij.be

antibot.hr

www.botfrei.de

Club R2GS

LSEC LEADERS IN SECURITY

10 YEARS

ACDC Online 1 : End User

Fighting botnets

www.botfree.eu

Connecting **users** to **solutions** through a set of European support centres

ACDC Online 2 : Project

www.acdc-project.eu

Operating as a European pilot project

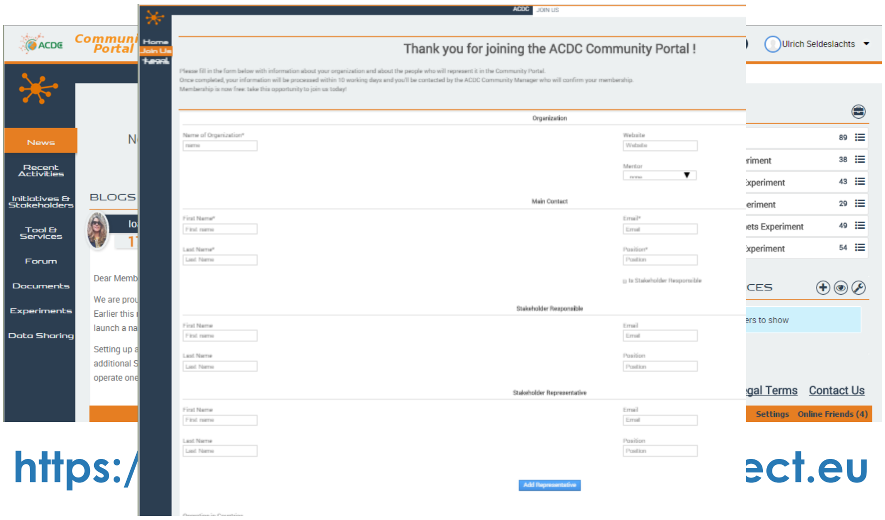
ACDC Online 3 : Community

- Operating as a community
- Joining forces to fight botnets

- Sharing intelligence
- Learning from tools & technologies and effects
- Expert network

https://communityportal.acdc-project.eu

ACDC Online 3 : Community



Dear Memb

We are prou
Earlier this
launch a na

Setting up a
additional S
operate one

Thank you for joining the ACDC Community Portal !

Please fill in the form below with information about your organization and about the people who will represent it in the Community Portal.
Once completed, your information will be processed within 10 working days and you'll be contacted by the ACDC Community Manager who will confirm your membership.
Membership is now free: take this opportunity to join us today!

Organization

Name of Organization* name

Website Website

Mentor

Main Contact

First Name* First name

Email* Email

Last Name* Last Name

Position* Position

□ Is Stakeholder Responsible

Stakeholder Responsible

First Name First name

Email Email

Last Name Last Name

Position Position

Stakeholder Representative

First Name First name

Email Email

Last Name Last Name

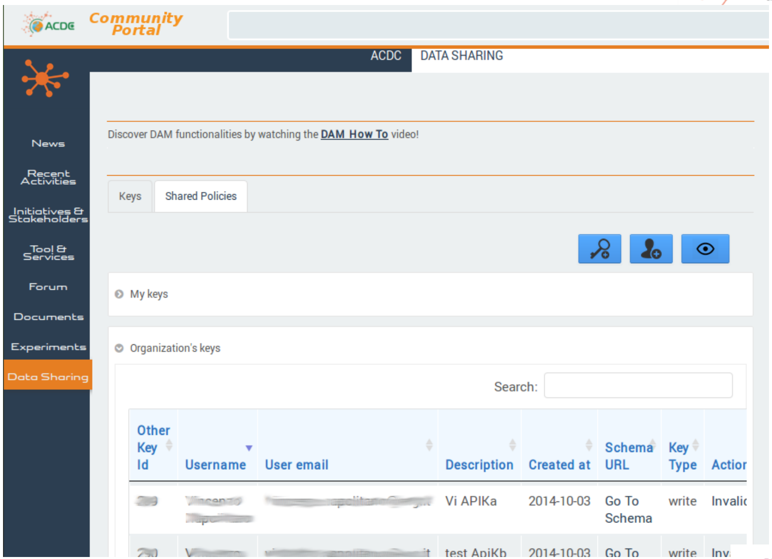
Position Position

Operating in Countries

https:/ ect.eu

ACDC Online 4 : Future CCH Connection

ACDC the Advanced Cyber Defence Centre



Discover DAM functionalities by watching the DAM How To video!

Keys | Shared Policies

My keys

Organization's keys

Search:

Other Key Id	Username	User email	Description	Created at	Schema URL	Key Type	Actior
[redacted]	[redacted]	[redacted]	Vi APIKa	2014-10-03	Go To Schema	write	Invalic
[redacted]	[redacted]	[redacted]	test ApiKb	2014-10-03	Go To	write	Inv

ACDC Online 3 : Community

ACDC the Advanced Cyber Defence Centre

EUROPOL

MONTENEGRO Computer Incident Response Team
CIRT

Authority for Consumers & Markets

Posteitaliane

CSIRT.SK
www.csirt.gov.sk

Internet Security Days

Centrale d'enregistrement et d'analyse pour la sûreté de l'information
MELANI

National Coordinator for Security and Counterterrorism
Ministry of Security and Justice

ZSIS

ACDC Online 3 : Community

ugr Universidad de Granada
HPI Hasso Plattner Institut
Hrvatski Telekom
Avira
Dutch Hosting Provider Association
cyscon
MACCSA
abuse information exchange
F-Secure
TREND MICRO
nsn

About LSEC

About LSEC & the Belgian R2GS Chapter

Ulrich Seldeslachts ,
Paris, December 17th, 2014

© Leaders in Security – LSEC, 2014, Public – Closed User Group Distribution, p 69

LSEC LEADERS IN SECURITY

IPACSO AWARDS
INNOVATION FRAMEWORK FOR ICT SECURITY
EUROPEAN CYBER SECURITY AND PRIVACY INNOVATION AWARDS
LSEC
DIW BERLIN
RIHON
VASCO
espion

infosecurity.be BELGIUM

FIC 2015

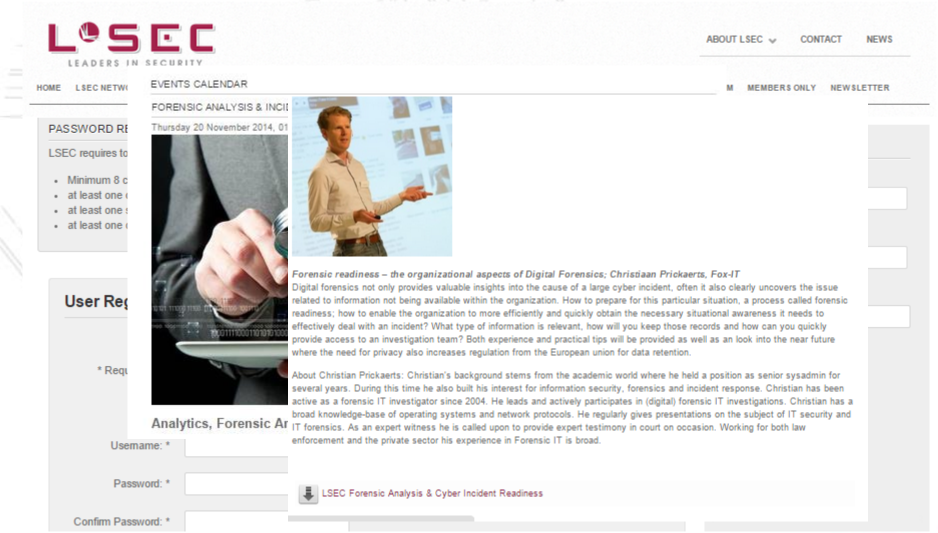
About LSEC Summary

1. Leaders In Security : a non-profit Flemish (vzw) industry association and user community supporting innovation & development of information security
   1. Data protection : protection of data, users, information and systems,
   2. Security management : standards, legal, good practices
   3. Tools and technologies : networking, encryption, virtualization
2. Over 135 members, e-security companies, reaching out to more than 25.000 ict professionals and security professionals, operations in Be, Nl, UK
3. Strategic partnes in ICT, TMT, Industry, Finance, Healthcare, Energy, … and in Germany, UK, Spain, France, Italy, Czech Republic, Ireland, US, …
4. Various international projects
   1. FIRE
   2. ACDC
   3. NEBUCOM
   4. IPACSO
   5. …
5. More than 100 activities per year in Belgium and abroad :
   1. Seminars, Conferences, trade shows, …
   2. www.lsec.be with over 5000 documents (white papers, business cases, presentations, … on information security related matters)
   3. Regular news letters, invitations, discussion for a

Key competences :

1. Dissemination - Outreach
2. End user relations
3. Business & Validation
4. Impact Coordination
5. Strategy & Innovation

Visit www.lsec.be for more information and documenation http://www.leadersinsecurity.org



Forensic readiness – the organizational aspects of Digital Forensics; Christiaan Prickaerts, Fox-IT

Digital forensics not only provides valuable insights into the cause of a large cyber incident, often it also clearly uncovers the issue related to information not being available within the organization. How to prepare for this particular situation, a process called forensic readiness; how to enable the organization to more efficiently and quickly obtain the necessary situational awareness it needs to effectively deal with an incident? What type of information is relevant, how will you keep those records and how can you quickly provide access to an investigation team? Both experience and practical tips will be provided as well as an look into the near future where the need for privacy also increases regulation from the European union for data retention.

About Christian Prickaerts: Christian's background stems from the academic world where he held a position as senior sysadmin for several years. During this time he also built his interest for information security, forensics and incident response. Christian has been active as a forensic IT investigator since 2004. He leads and actively participates in (digital) forensic IT investigations. Christian has a broad knowledge-base of operating systems and network protocols. He regularly gives presentations on the subject of IT security and IT forensics. As an expert witness he is called upon to provide expert testimony in court on occasion. Working for both law enforcement and the private sector his experience in Forensic IT is broad.

LSEC Forensic Analysis & Cyber Incident Readiness

NOT THE END

More information and follow-up

www.lsec.be

www.leadersinsecurity.org

Club R2GS

cloud security alliance CSA

European Commission

SEVENTH FRAMEWORK PROGRAMME

IWT

agentschap voor Innovatie door Wetenschap en Technologie

Flanders Investment & Trade

Q or C

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