computer
emergency
response
team

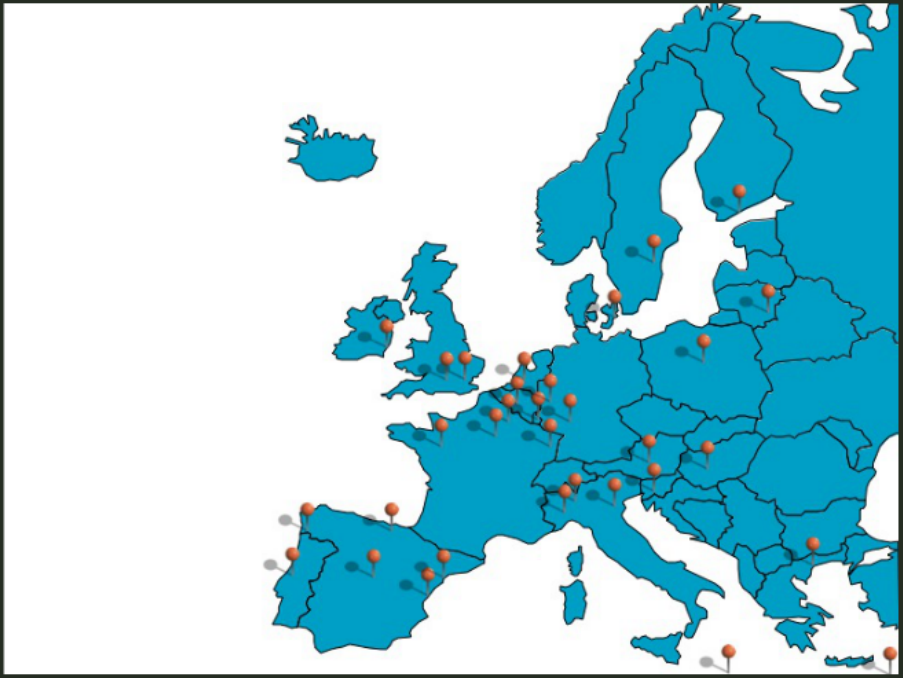
CERT-EU

for the EU institutions, bodies
and agencies

CERT for the EU institutions, bodies and agencies

- Pre-configuration team
- 60+ clients
- Resources made available by the clients
- Operational support
- Off-line
- Collaboration with internal ITsec teams
- Single point of contact
- European Digital Agenda

Clients



Partners

CERT

GOVCERT.NL

CPNI Centre for the Protection of National Infrastructure

CERT.at

CERT Bund

GovCertUK COMPUTER EMERGENCY RESPONSE TEAM

CERTA

CIRCL Computer Incident Response Center Luxembourg

NCIRC NATO COMPUTER INCIDENT RESPONSE CAPABILITY

cert-fi

CERT SE KONKURRENSNEUTRAL IT-SÄKERHET FÖR NÄRINGSLIV OCH OFFENTLIG SEKTOR

www mil .be

CERT.be

CERT Eesti Computer Emergency Response Team

CCN-CERT

CERT POLSKA

US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM

TEAM CYMRU COMMUNITY SERVICES

shadowserver

Microsoft Be what's next.

Google

Symantec. Confidence in a connected world.

McAfee An Intel Company

FCCU

EUROPOL

Office layout, walls, doors, carpet, painting

Furniture

Sunshield, sunblinds

Fridge, microwafe

Security doors, security locks

Intrusion detection, alarm, Videophone

Fire- and waterproof safe

Server room, airco, fire extinction, UPS

High speed direct internet connection

Servers, routers, firewalls, switches

Isolated local area network

Desktop computers, printers

Office automation software, email system

Help desk

Temporary server to host webportal

Photocopy, scanner, shredder

Beamer, projection screen

Videoconferencing

Functional mailbox, phone and smartphone

Recruitments (AD, END)

Service passes, SYSPER

Mission and training budget

Small procurement budget

Business cards

EUROPA page, guide des services

Webportal EMM, sources, keywords

Logo and graphical image

PGP, ACID, CHIASMUS, SECEM

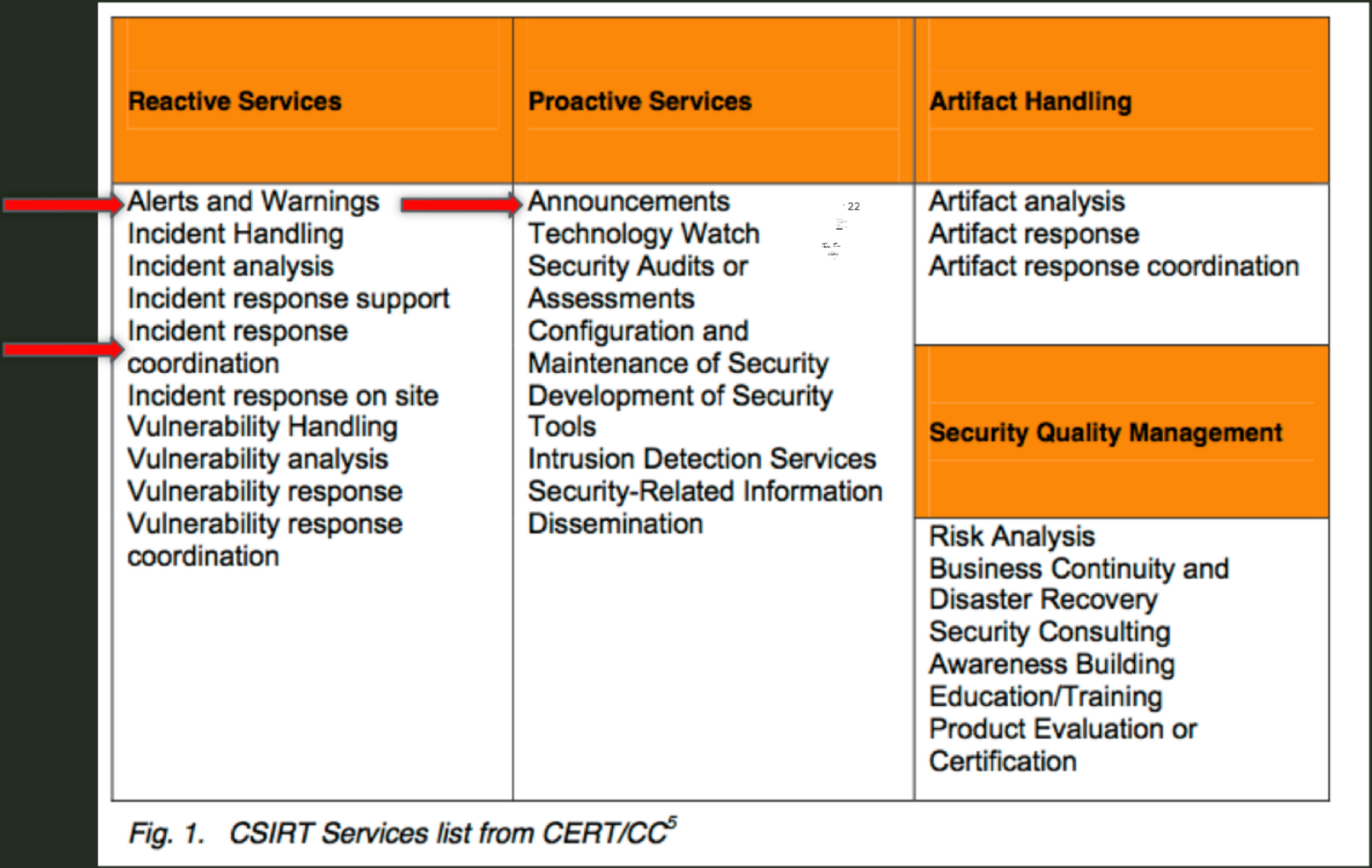
Domain name

Name registration

Created 1/6/2011

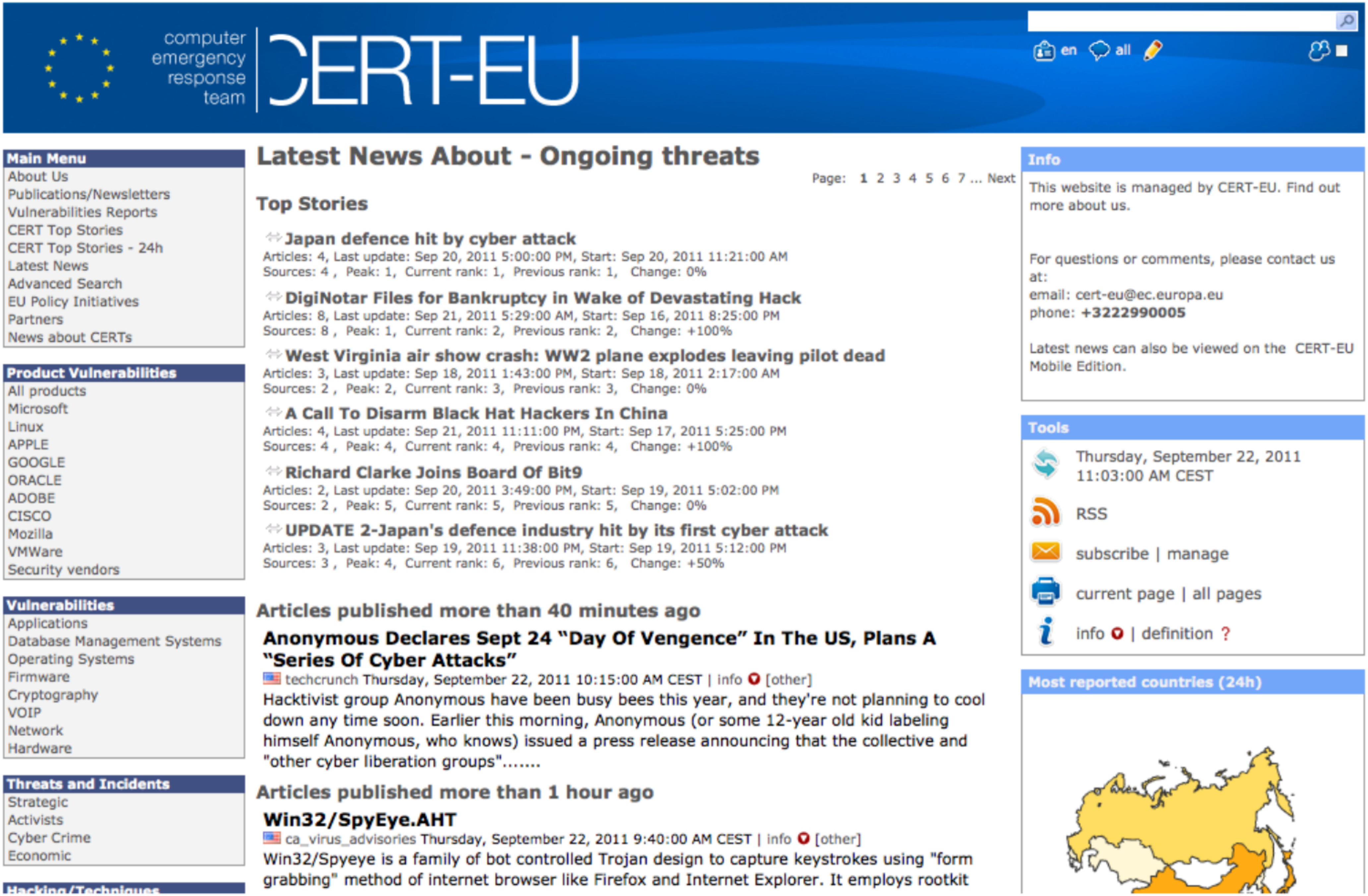
- 10/5: go ahead
- 13/5: recruitment interviews
- 20/5: premises made available
- 14/6: revamping of offices finished
- 14/6: furniture and office computers installed
- July: design web portal
- July: client survey
- July-September: meetings with 15 CERTs
- August: construction of server room
- August: design of graphical identity
- 15/8 and 1/9 arrival of new staff
- 15/9: installaction of servers
- 20/9: dry run of web portal
- 22/9: official inauguration

Services to be offered by pre-configuration team



Reactive Services	Proactive Services	Artifact Handling
Alerts and Warnings Incident Handling Incident analysis Incident response support Incident response coordination Incident response on site Vulnerability Handling Vulnerability analysis Vulnerability response Vulnerability response coordination	Announcements Technology Watch Security Audits or Assessments Configuration and Maintenance of Security Development of Security Tools Intrusion Detection Services Security-Related Information Dissemination	Artifact analysis Artifact response Artifact response coordination
		Security Quality Management
		Risk Analysis Business Continuity and Disaster Recovery Security Consulting Awareness Building Education/Training Product Evaluation or Certification

Fig. 1. CSIRT Services list from CERT/CC[5]



computer emergency response team CERT-EU

en | all

Main Menu
- About Us
- Publications/Newsletters
- Vulnerabilities Reports
- CERT Top Stories
- CERT Top Stories - 24h
- Latest News
- Advanced Search
- EU Policy Initiatives
- Partners
- News about CERTs

Product Vulnerabilities
- All products
- Microsoft
- Linux
- APPLE
- GOOGLE
- ORACLE
- ADOBE
- CISCO
- Mozilla
- VMWare
- Security vendors

Vulnerabilities
- Applications
- Database Management Systems
- Operating Systems
- Firmware
- Cryptography
- VOIP
- Network
- Hardware

Threats and Incidents
- Strategic
- Activists
- Cyber Crime
- Economic

Hacking/Techniques

Latest News About - Ongoing threats

Page: 1 2 3 4 5 6 7 ... Next

Top Stories

Japan defence hit by cyber attack
Articles: 4, Last update: Sep 20, 2011 5:00:00 PM, Start: Sep 20, 2011 11:21:00 AM
Sources: 4 , Peak: 1, Current rank: 1, Previous rank: 1, Change: 0%

DigiNotar Files for Bankruptcy in Wake of Devastating Hack
Articles: 8, Last update: Sep 21, 2011 5:29:00 AM, Start: Sep 16, 2011 8:25:00 PM
Sources: 8 , Peak: 1, Current rank: 2, Previous rank: 2, Change: +100%

West Virginia air show crash: WW2 plane explodes leaving pilot dead
Articles: 3, Last update: Sep 18, 2011 1:43:00 PM, Start: Sep 18, 2011 2:17:00 AM
Sources: 2 , Peak: 2, Current rank: 3, Previous rank: 3, Change: 0%

A Call To Disarm Black Hat Hackers In China
Articles: 4, Last update: Sep 21, 2011 11:11:00 PM, Start: Sep 17, 2011 5:25:00 PM
Sources: 4 , Peak: 4, Current rank: 4, Previous rank: 4, Change: +100%

Richard Clarke Joins Board Of Bit9
Articles: 2, Last update: Sep 20, 2011 3:49:00 PM, Start: Sep 19, 2011 5:02:00 PM
Sources: 2 , Peak: 5, Current rank: 5, Previous rank: 5, Change: 0%

UPDATE 2-Japan's defence industry hit by its first cyber attack
Articles: 3, Last update: Sep 19, 2011 11:38:00 PM, Start: Sep 19, 2011 5:12:00 PM
Sources: 3 , Peak: 4, Current rank: 6, Previous rank: 6, Change: +50%

Articles published more than 40 minutes ago

Anonymous Declares Sept 24 "Day Of Vengence" In The US, Plans A "Series Of Cyber Attacks"

techcrunch Thursday, September 22, 2011 10:15:00 AM CEST | info | [other]

Hacktivist group Anonymous have been busy bees this year, and they're not planning to cool down any time soon. Earlier this morning, Anonymous (or some 12-year old kid labeling himself Anonymous, who knows) issued a press release announcing that the collective and "other cyber liberation groups".......

Articles published more than 1 hour ago

Win32/SpyEye.AHT

ca_virus_advisories Thursday, September 22, 2011 9:40:00 AM CEST | info | [other]

Win32/Spyeye is a family of bot controlled Trojan design to capture keystrokes using "form grabbing" method of internet browser like Firefox and Internet Explorer. It employs rootkit

Info

This website is managed by CERT-EU. Find out more about us.

For questions or comments, please contact us at:
email: cert-eu@ec.europa.eu
phone: **+3222990005**

Latest news can also be viewed on the CERT-EU Mobile Edition.

Tools

Thursday, September 22, 2011
11:03:00 AM CEST

RSS

subscribe | manage

current page | all pages

info | definition ?

Most reported countries (24h)

CERT-EU

Latest News About - Ongoing threats

Top Stories

Japan defence hit by cyber attack

A Call To Disarm Black Hat Hackers In China

Articles published more than 48 minutes ago

Anonymous Declares Sept 24 "Day Of Vengeance" In The US, Plans A "Series Of Cyber Attacks"

Articles published more than 1 hour ago

CERT-EU webportal

- 800+ sources
- Automatic scraping of relevant news
- Categorisation and clustering
- Next step: html5

EMM Private

- Underground sources
- Authoring access for other CERTs

http://cert.europa.eu/

Advisories

2011 (Sept – Dec)	33
1Q2012	46
2Q2012	22

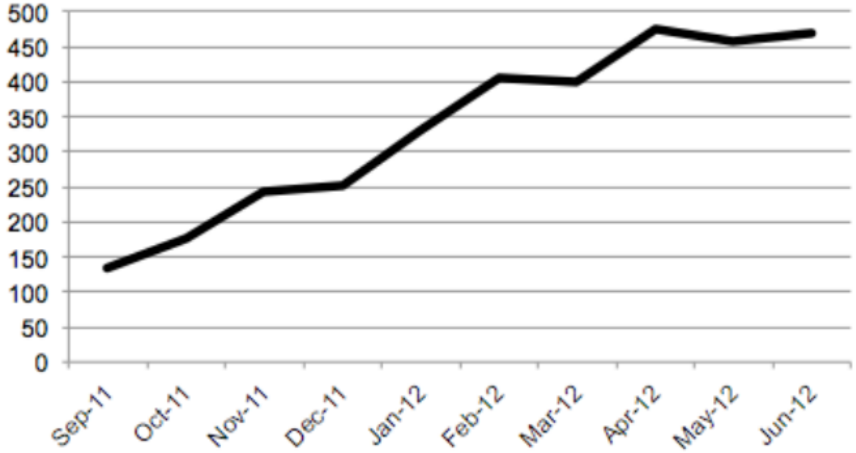
- Sources: EMM, mailing lists
- Subjects: vulnerabilities, generic threats

Alerts

2011 (Sept – Dec)	50
1Q2012	154
2Q2012	122 (49)

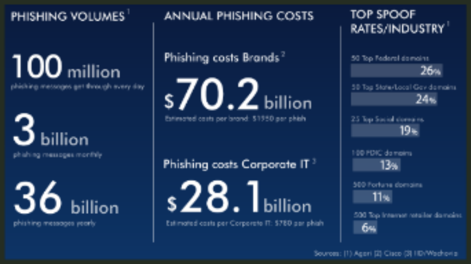
- Sources: Customers (incidents), CERTs (alerts), passive monitoring
- Subjects: compromised systems, immediate threats

Average number of unique visitors per day



Most frequent infection vectors

- Infected USB sticks
- XSS/SQL injection
- Web browsing
- Emails (attachments, links)



PHISHING VOLUMES[1]

100 million
phishing messages get through every day

3 billion
phishing messages monthly

36 billion
phishing messages yearly

ANNUAL PHISHING COSTS

Phishing costs Brands[2]

$70.2 billion
Estimated costs per brand: $1550 per phish

Phishing costs Corporate IT[3]

$28.1 billion
Estimated costs per Corporate IT: $780 per phish

TOP SPOOF RATES/INDUSTRY[1]

50 Top Federal domains	26%
50 Top State/Local Gov domains	24%
25 Top Social domains	19%
100 FDIC domains	13%
500 Fortune domains	11%
500 Top Internet retailer domains	6%

Sources: (1) Agari (2) Cisco (3) IID/Wachovia

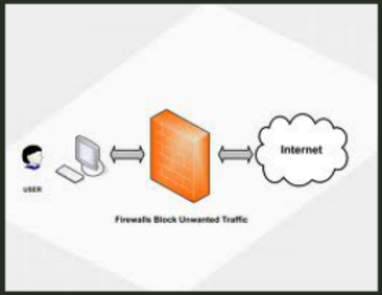
Extent of the problem not clear to the constituent

- Hidden in the noise of spam
- Lack of user awareness
- Lack of internal reporting mechanisms
- Lack of tools to analyse emails (extraction, testing of links and attachments)

Problems with targeted attacks

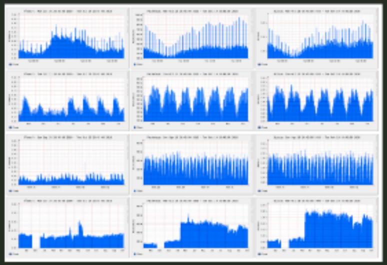
- Undetected by the protection systems
- IT department underestimates the problem
- Highly specialised resources to analyse the problem
- Fear of informing hierarchy
- Fear of involving law enforcement
- Difficult to perform the attribution
- Difficult to demonstrate the damage
- Never sure if the problem is resolved

Detection



Client

- Multiple A/V systems
- Additional systems scans
- Network protection systems
- Log analysis
- User awareness (anomalies)



CERT-EU + partners

- Passive malevolence monitoring
- TLD website monitoring
- Mail scanner
- CIMBL

Containment

Client

- Set up reaction team
- Call in the experts
- Isolate compromised system
- Forensic image
- Analyse logs
- Scan other systems
- Assess potential impact on information
- Inform other concerned parties
- Involve LE?

CERT-EU + partners

- Forensic imaging guidelines
- CERT Toolbox
- Interpret and advise

Eradication

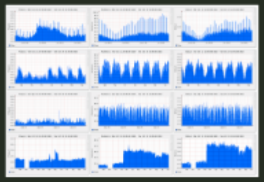
Client

- Reimage infected or suspected systems
- Reset passwords (all at the same time)
- Reset passwords in external accounts
- Rescan (regularly)
- Analyse logs (regularly)

CERT-EU + partners

- Analyse malware
- Interpret and advise
- Inform other constituents
- Inform other CERTs

Prevention



Clients

- Risk assessment of information assets (value / risk)
- Information security policy
- Perimeter protection (IDS, AV, WAF) and segmentation
- Log analysis in/out/internal -> anomalies?
- User and password management
- Version and patch management
- Regular scans (MSS)
- Embed security in the application development
- Deactivate autorun (Windows XP), upgrade to Windows 7 - enforcement of policies
- User awareness

CERT-EU

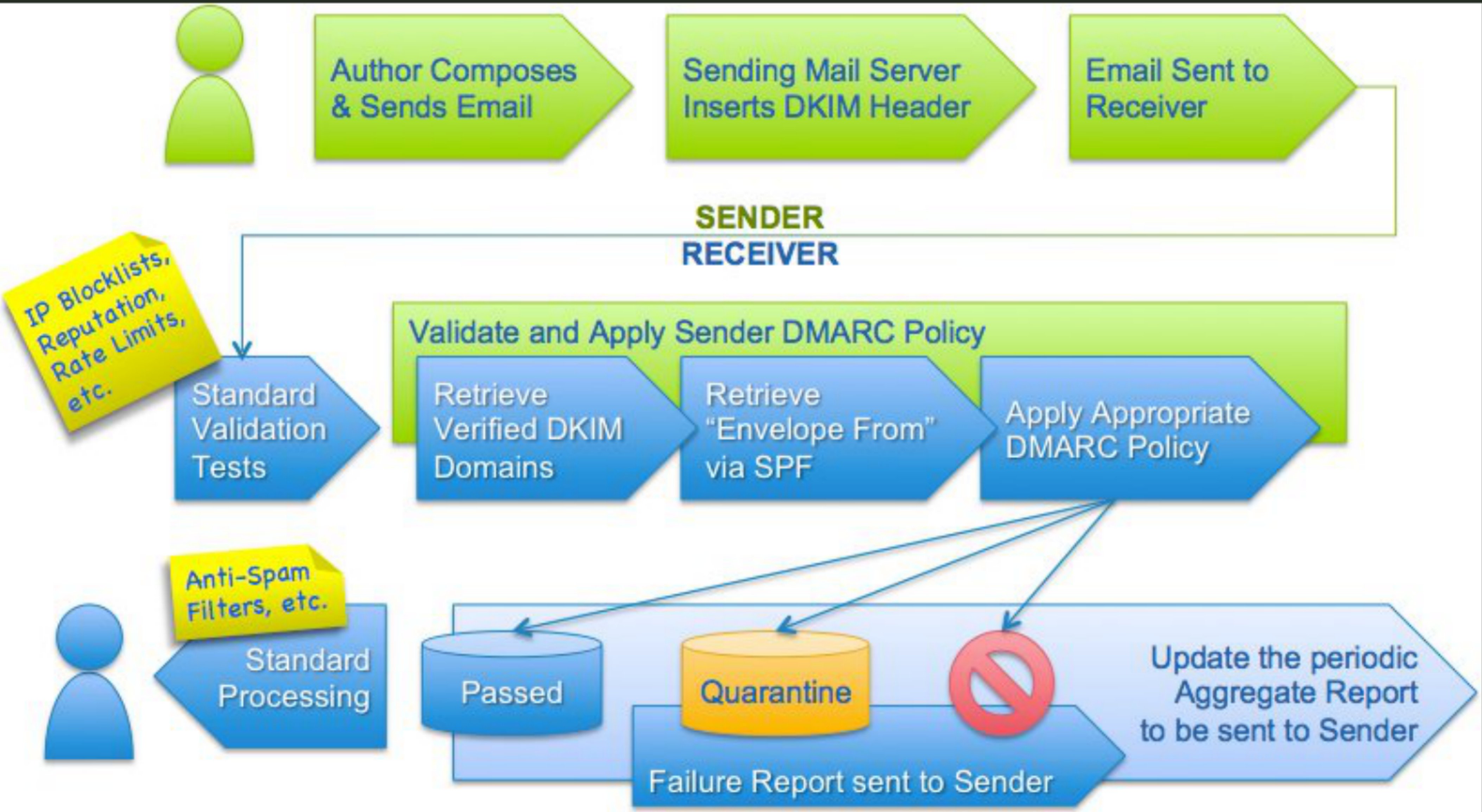
- Advisories and white papers
- Client specific advise and consultancy
- Awareness raising and training material

Tools for detection

- Cymru, Shadowserver, Arbor, N6
- Microsoft / Google
- AbuseHelper
- Pastebin scanning
- Mail scanner / analyser

Next steps

- More sources
- IDS sensors (SNORT / third party)
- DMARC



Author Composes & Sends Email

Sending Mail Server Inserts DKIM Header

Email Sent to Receiver

SENDER

RECEIVER

IP Blocklists, Reputation, Rate Limits, etc.

Standard Validation Tests

Validate and Apply Sender DMARC Policy

Retrieve Verified DKIM Domains

Retrieve "Envelope From" via SPF

Apply Appropriate DMARC Policy

Anti-Spam Filters, etc.

Standard Processing

Passed

Quarantine

Update the periodic Aggregate Report to be sent to Sender

Failure Report sent to Sender

Malware analysis

- Small internal capacity
- Expertise in clients (EC, GSC)
- Other CERTs
- IT sec partners

Systems

- Internal infrastructure being built up
- System for information sharing on non-public malware
- Automated tools (EC, VirusTotal)

Broader issues

- "Industrial-scale" detection of anomalies
  - Capitalise on existing capacities
  - Foster open exchange of data on indicators of malevolence
- "Industrial" exchange and protection mechanisms
  - Standardisation of meta-data
  - Automated upload in network protection - ISP and network borders
  - Systems and tools for trusted information exchange on incidents, malware

- More effective collaboration between CERTs
  - Sharing of validated IOCs in a standardised format
  - Sharing of information on critical incidents -

- Reporting compromises to individuals, SMEs, cross-sector

- "Break the silence", everybody is suffering targetted attacks
- "Break the silos", sharing between CERTs, LE, intell

- Aim for consolidated, validated, up-to-date data set of IOC

Outlook CERT-EU

Challenges

- User awareness / internal processes to handle anomalies
- Better information sharing by clients
- Better responsiveness of clients to alerts
- Better automated detection mechanisms, more sources
- Automated protection processes

Next steps

- More capacity in alerting and incident handling
- Basic artifact analysis capacity
- More client-specific service
- Broader and modular service package, including network sensors for some clients requesting such service
- Systems and tools development in particular for "industrial" detection of anomalies and exchange of information

Thank You

http://cert.europa.eu/