Cybercrime : a CERT perspective

> I/ CERTs
>II/ Risks
>III Responses

V1.0

LEXSI
INNOVATIVE SECURITY

I/ Types of CERTs

Nomenclature

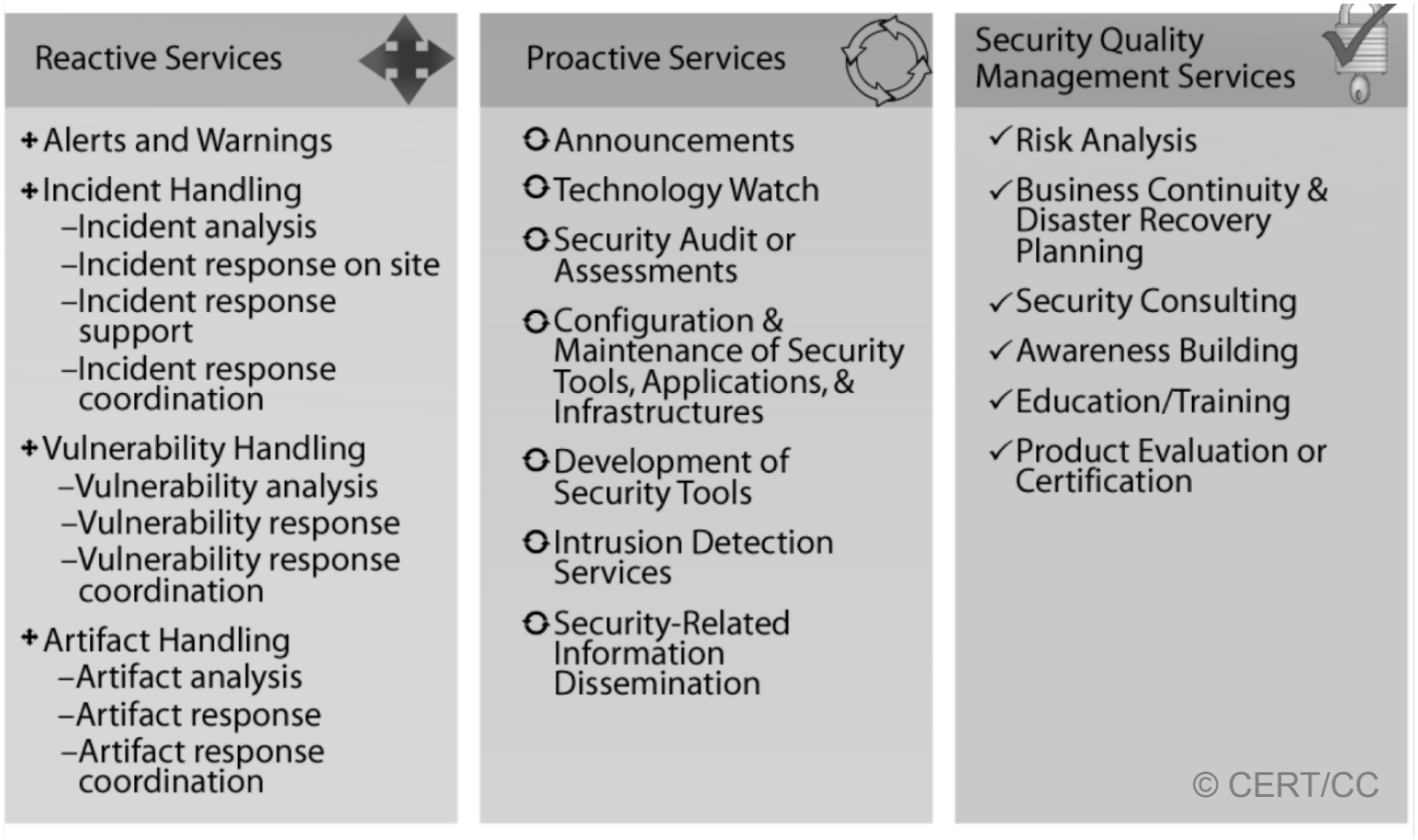
- CERT (Computer Emergency Response Team)

= CSIRT (Computer Security Incident Response Team)

Typology => Constituency

- ✓ Internal
- ✓ National
- ✓ Sector (i.e. Government, Military, Academics, Finance, etc.)
- ✓ Private
- ✓ Vendor (PSIRT: Product Security Incident Response Team)

I/ How CERTs can help

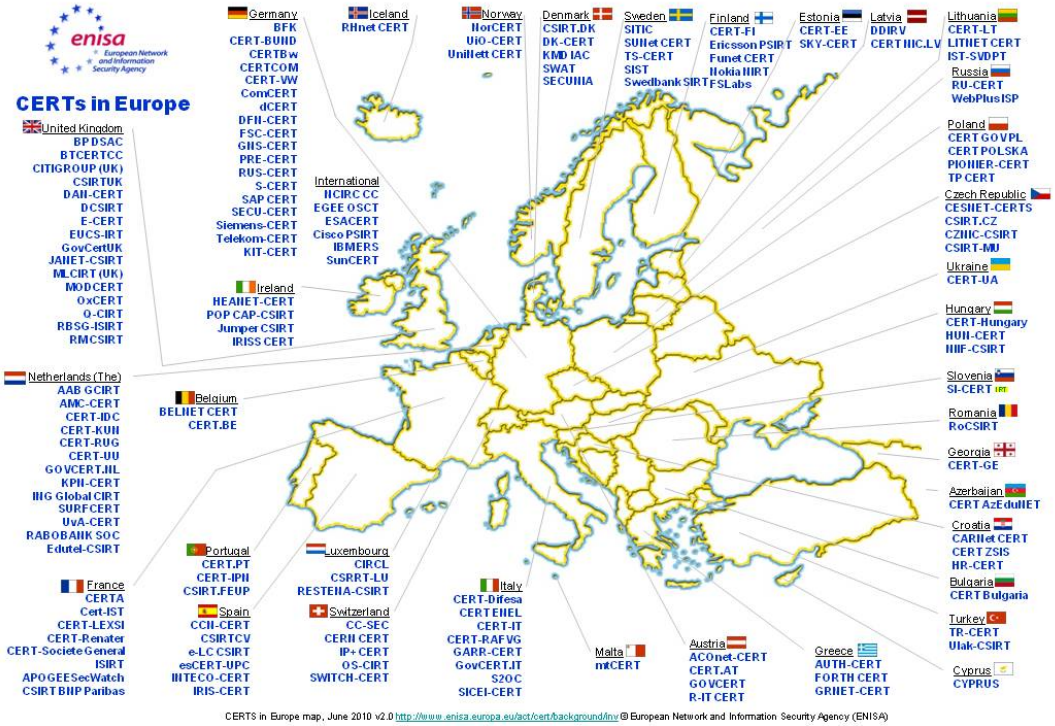


CERTs HELP LOWER THE EFFECTS,
NOT TACKLE THE ROOTS OF CYBERCRIME

I/ CERTs key asset : cooperation

Trusted cooperation networks for information exchange and early warnings :

> Geographic
> Industry
> Typology
> Shared interests



FIRST
TRUSTED Introducer
APCERT
EGC group
OIC-CERT Computer Emergency Response Team

II/ Risks: Breakdown of cybercriminals motives

Threats \ Motivations	Personal	Political	Image	Money
Hacktivism	X	X	X	
Cyber-bullying	X			
Child Abuse	X			(X)
Fraud				X
Espionage		X		X
Sabotage / Disruption	X	X	X	X
Deception	X	X	X	X

II/ Risks: Vectors leveraged by cybercriminals

TECHNICAL	ENVIRONMENTAL
Do-It-Yourself exploits, phishing kits	Social engineering
Insecure coding (protocols, OS, applications, etc.)	Growth of Internet users + bandwidth
Mobile devices	Economic crisis
Social networks platforms	Mixed personal/professional Internet uses
P2P sharing	Worldwide competition
Underground forums/market places	Anonymity (surf, money flows, encrypted communications, domain registration, etc.)
Weak authentication	Password re-use
…	…

III/ Preventive responses

- ✓ **Solve PPP issues**
  - ✓ Information sharing vs. Privacy
  - ✓ One-way information flow (Private -> Public)
  - ✓ Incident reporting standards / formats
- ✓ **Boost awareness raising**

  But long term effort, with relative low ROI

  (How successful have we been on:

  Threats: spam, scam, phishing, rogue AV ?

  Technologies: Wi-Fi, AV updates, social networks, smartphones?)
- ✓ **Promote secure coding contracting**

  Regulation or incentives ?

III/ Reactive responses : disrupt cybercriminals (1)

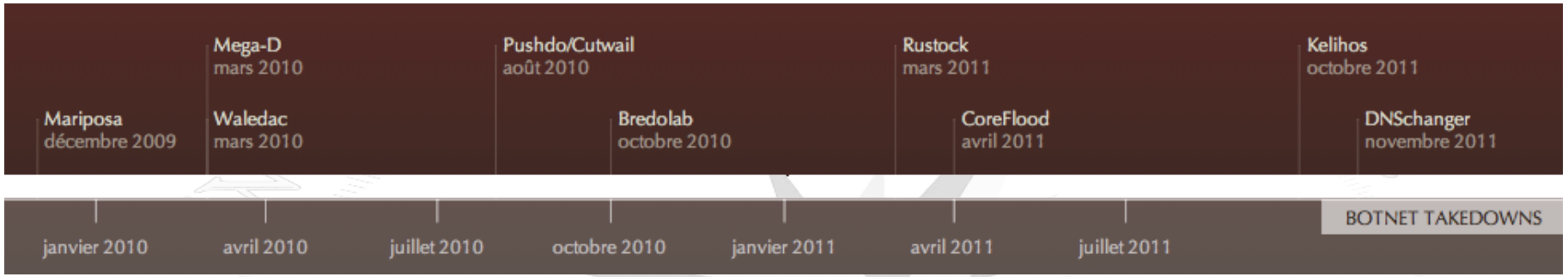
- ✓ **Clean / block malicious resources**
  - ✓ URLs, domains, IP, etc.

- ✓ **Take down specific fraudulent providers**
  - ✓ bulletproof hosting providers (RBN, McColo, 3FN, Troyak, etc.)
  - ✓ fraudulent registrars (EstDomains)

BUT : new solutions are quickly developed by bad guys

- IP (fast-flux)
- Spam (ESP breaches, social networks)
- Hosting (BGP over VPN, DNS tunnelling)
- etc.

III/ Reactive responses : disrupt cybercriminals (2)



- ✓ **Mitigating botnets**
  - ✓ Cleaning / Help desk center (DE, JP)
  - ✓ Takedown (Microsoft, US/NL/SP LEAs)

BUT: no bots shortage

- 1,000 bots for 4 to 20$ (depending on country)
- +10,000 bots in a few hours using spam or drive-by-download
- (4-6M bot infections/month according to McAfee)

EXPLOIT KITS

III/ Industry responses : pushing self-regulation

- ✓ **Naming and shaming**
  - ✓ Spammers (SpamHaus ROKSO)
  - ✓ Hosting Providers / ISPs (HostExploit-SiteVet)
  - ✓ SCADA vendors (Insecure Product List)
  - ✓ Banking industry (i.e. online pharmacies : UCSD)
  - ✓ Registries, registrars, etc.

BUT: whac-a-mole game

- ✓ **Voluntary code of conduct**
  - ✓ ISPs (botnets) : in effect (NL, AUS, JP) or discussed (US)
  - ✓ Email Marketing (spam) : FR, CA, etc.

BUT: incentives vs. additional costs/impacts on revenue

III/ Regulatory & legal responses

- ✓ **Update and harmonize legal & regulatory frameworks**
  - ✓ Product certification
  - ✓ Industry standards / compliance

    Finance (i.e. PCI-DSS, EMV, 2FA, etc.)

    ISPs (botnets in Finland, data breach notification in EU)

BUT: often confused with security (check-list syndrom)

  - ✓ Multi-national laws / treaties (EU, COE)
  - ✓ Cyberwar rules of engagement (nation-states attacks)

BUT: slow process, political/diplomatic agendas, etc.

III/ Judicial responses

✓ **Empower your High-Tech Crime Law Enforcement Units**

(staff, training & exercises, tools, cooperation processes, etc.)

✓ **Effectively prosecute cybercriminals**

Trust your foreign counterparts

=> Make cybercrime a riskier, less attractive business !

Thank You !

CERT- LEXSI
cert.lexsi.com
cert-soc@lexsi.com
+33.810336060