



# CERT-LEXSI Update

CERT-LEXSI

06/02/2012



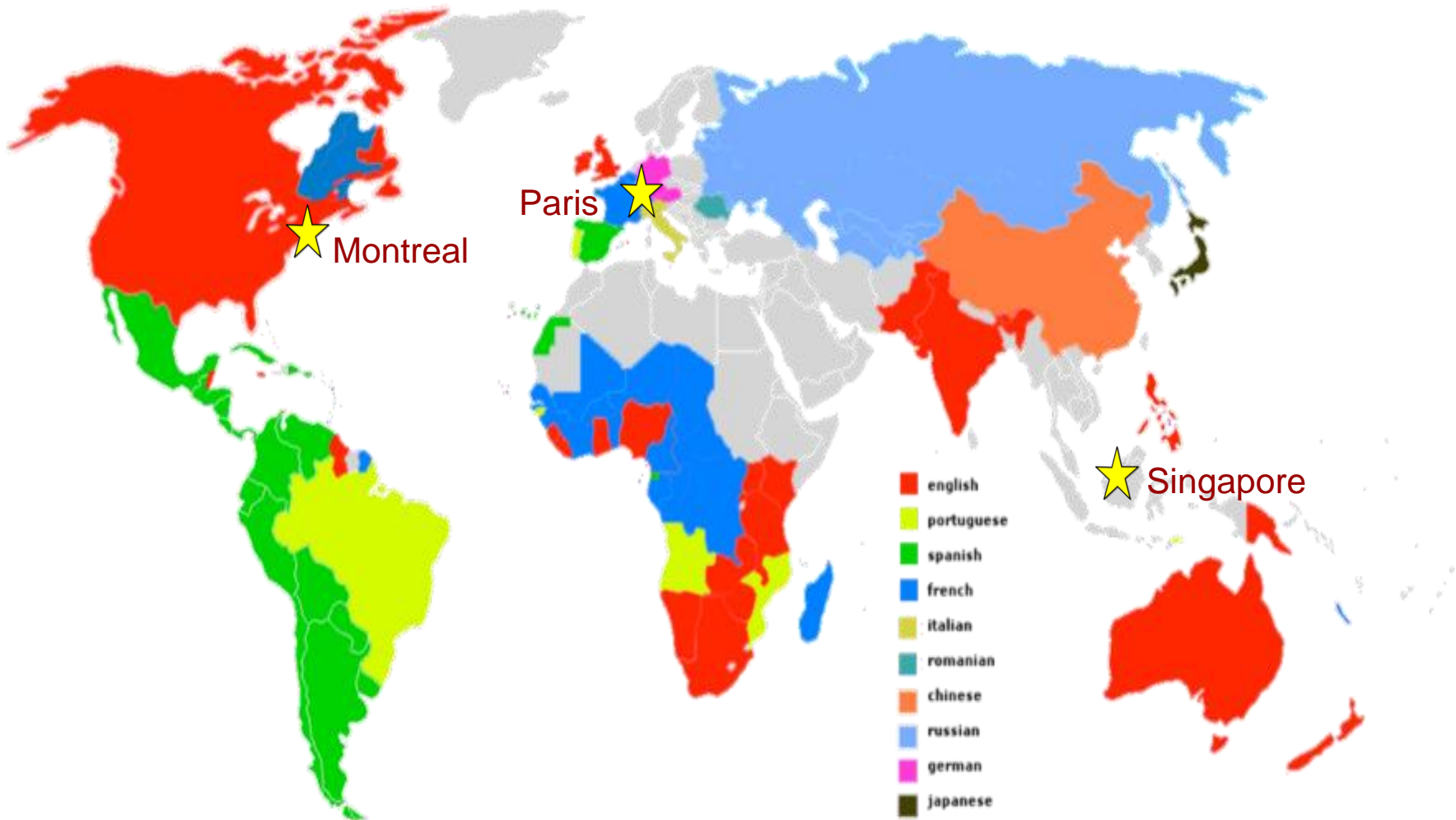
# CERT-LEXSI Presentation

1. Independent Service Provider Customer Base CSIRT team in France established in 2001
2. 34 (+4) Multilingual Team
3. Our services are available on:
  - A basic schedule : Monday to Friday, 9hr to 19hr
  - An extended schedule : 7hr30 to 20hr30
  - 24/7/365
4. Network of strong relationships (LEAs, CSIRTs, Editors, etc.)
5. Accredited in 2009 by Trusted Introducer into TF-CSIRT
6. Authorized “CERT” User by CERT® Coordination Center (CERT/CC)
7. Member of several Working Groups (SignalSpam, Phishing-Initiative, etc.)



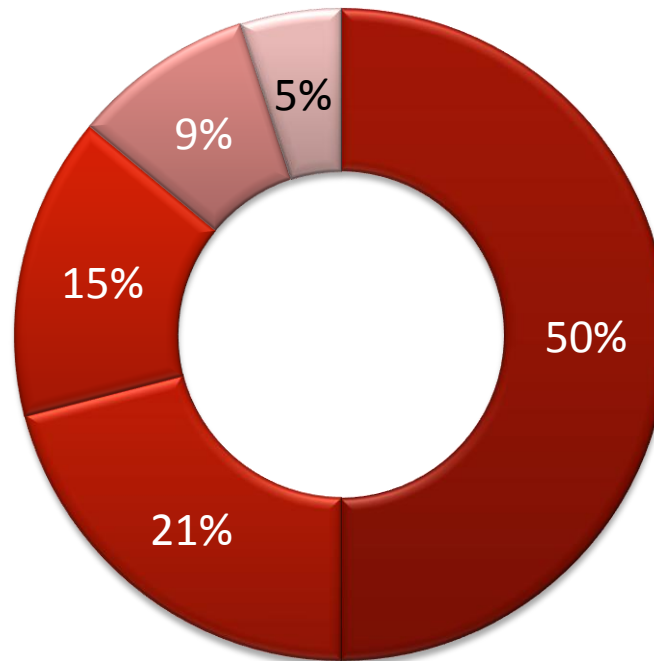
# CERT-LEXSI 24/7

## Linguistic Coverage of CERT-LEXSI



# CERT-LEXSI Constituency

- Banking - Assurance
- Industry - Energy -Utilities
- Services - Transports - Distribution
- Public
- Télécoms



# CERT-LEXSI Services

Our direct CSIRT-related activities for our constituency:

- Incident Response (Forensics, RCE, DDoS)
- Cybercrime detection, investigation and mitigation
  - Phishing, malware, domains, profiling, studies
- Vulnerability management (vulnerability database and alerting)
- IT products stressing (fuzzing, RCE, code audit)
- Awareness and training





# CERT-LEXSI 2011 Projects

- Malware Analysis Sandboxes (Android, iPhone)
- Malware day to day monitoring platform
- Hacktivism & Malware Data Leakage Detection
- “so-called” APTs
- Building Internal CSIRTs

# CERT-LEXSI Main Issues

- 2008: 100 Phishing Countermeasures -> 2011: **10.000** !
- How to deal with Smartphone's security and monitoring ? (iPhone iOS emulation, Android Market / AppStore apps fluxes)
- Heterogeneous & large constituency -> Less visibility (no IRT)

**CERT-LEXSI**

**<https://cert.lexsi.com/weblog>**

**[cert@lexsi.com](mailto:cert@lexsi.com)**

**+33 810 33 60 60**