IRMA

Incident Response & Malware Analysis

Alexandre Quint

SSTIC14 – Rump Session – 05/06/14

Your own personal multi-analysis engine

- Analyse de fichiers (Antivirus, Hashdb, Analyse statique, Sandbox …)
- Utilisation en mode public ou privé
- Contrôle des fichiers analysés

INNOVATIVE SECURITY

Cofinancement

AIRBUS GROUP

DE LA RECHERCHE À L'INDUSTRIE
cea

GRAND DUCHY OF LUXEMBOURG
GOVCERT.LU

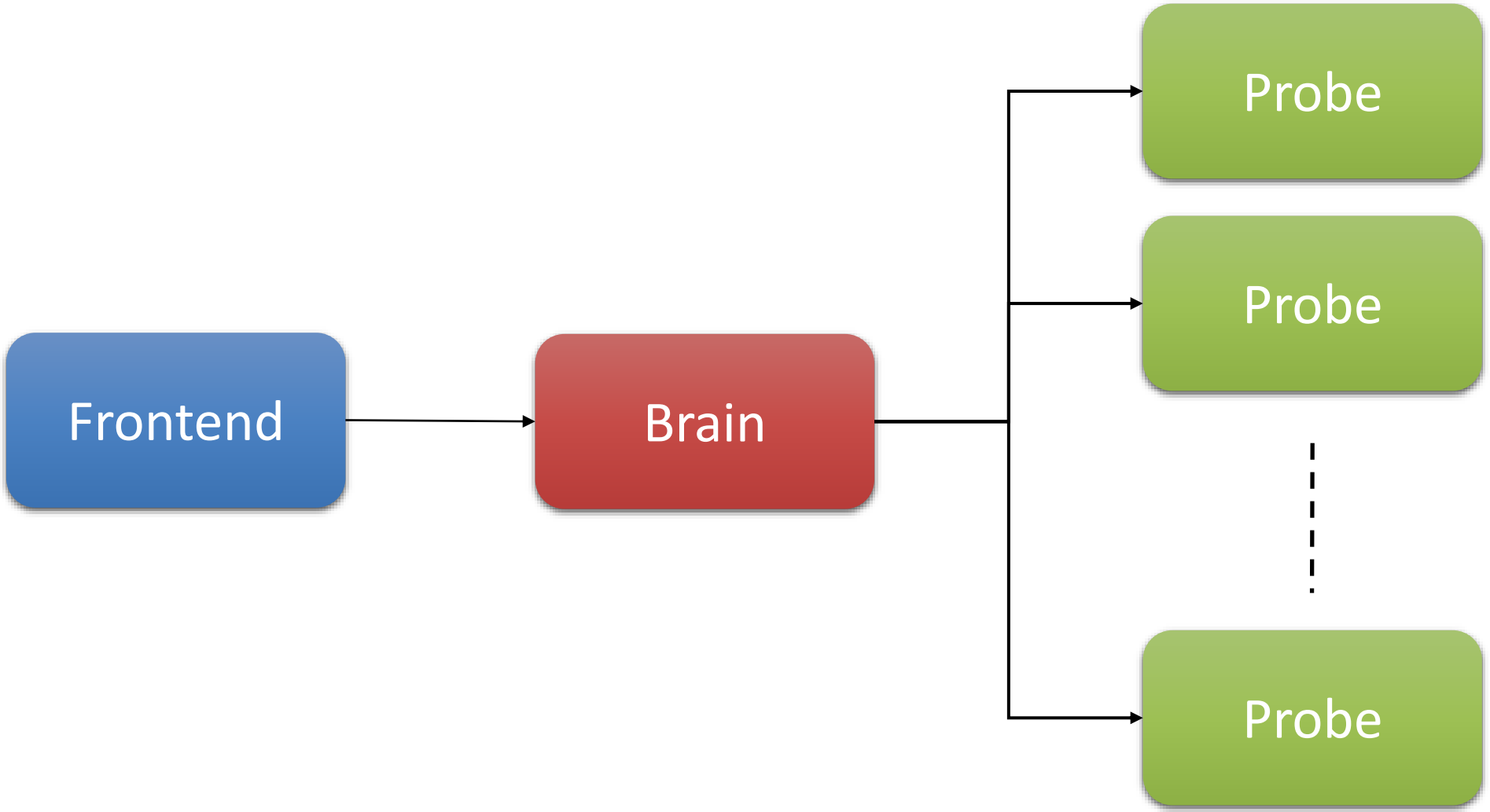
orange™

DCNS

INNOVATIVE SECURITY

INNOVATIVE SECURITY

Macro Architecture



INNOVATIVE SECURITY

Featuring


NGINX


Bottle


mongoDB


python™


C


Qemu


libvirt
VIRTUALIZATION API


RabbitMQ™
Messaging that just works


INNOVATIVE
SECURITY

Disponible sous licence Apache 2.0

https://github.com/quarkslab/irma-frontend
https://github.com/quarkslab/irma-brain
https://github.com/quarkslab/irma-probe

INNOVATIVE SECURITY

Installation

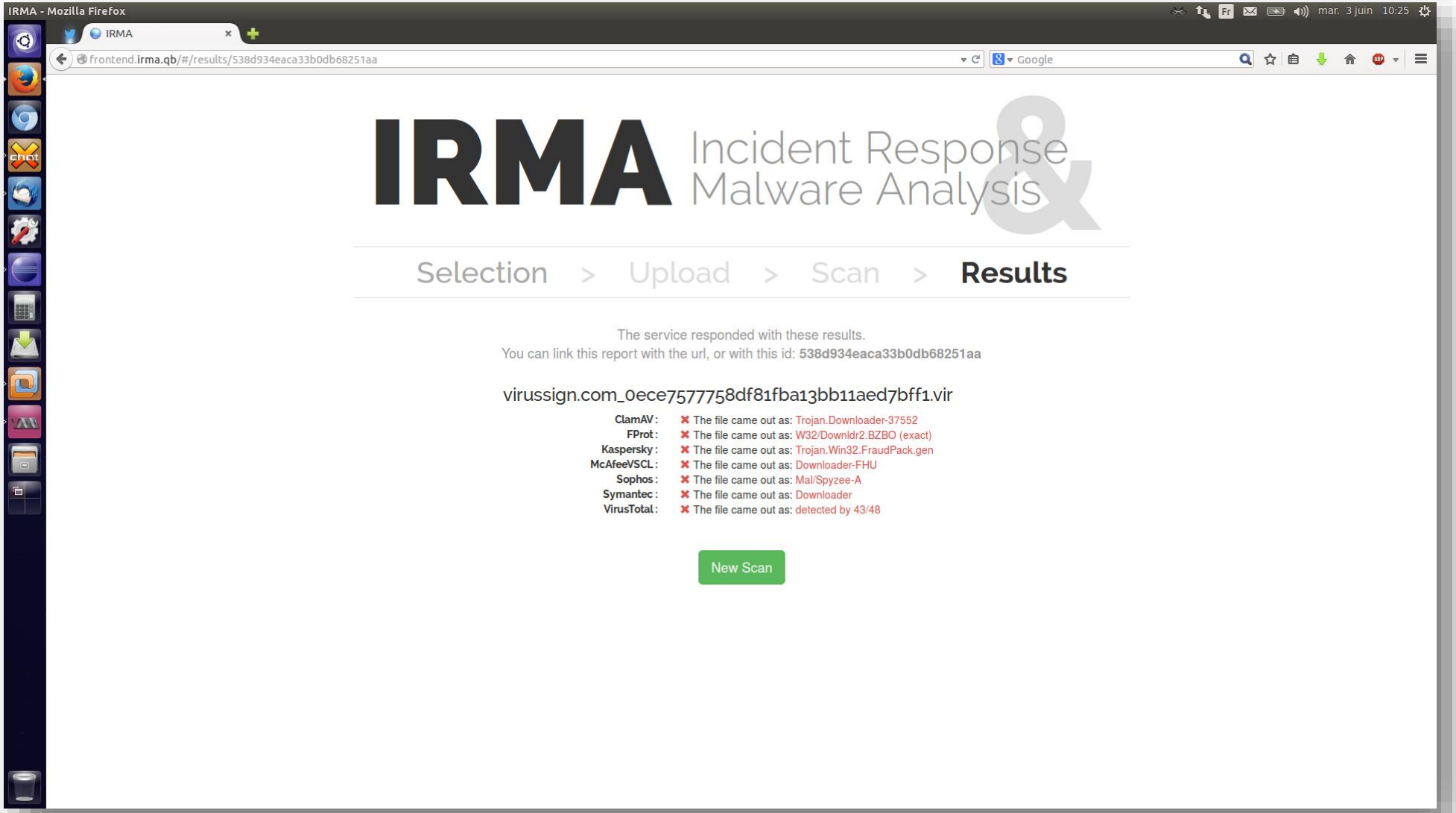
Rôle	Package	OS testé(s)
Frontend	pip / deb	Debian stable
Brain	pip / deb	Debian stable
Probe	pip only	Debian stable Win7

INNOVATIVE SECURITY

Démo time

INNOVATIVE SECURITY

Démo printf (1/2)



INNOVATIVE SECURITY

Démo printf (2/2)

The service responded with these results.

You can link this report with the url, or with this id: **538d934eaca33b0db68251aa**

virussign.com_0ece7577758df81fba13bb11aed7bff1.vir

ClamAV :	✖ The file came out as: Trojan.Downloader-37552
FProt :	✖ The file came out as: W32/Downldr2.BZBO (exact)
Kaspersky :	✖ The file came out as: Trojan.Win32.FraudPack.gen
McAfeeVSCL :	✖ The file came out as: Downloader-FHU
Sophos :	✖ The file came out as: Mal/Spyzee-A
Symantec :	✖ The file came out as: Downloader
VirusTotal :	✖ The file came out as: detected by 43/48

New Scan

INNOVATIVE SECURITY

Contact / Questions ?

@qb_irma

IRC #qb_irma@freenode

David Carle dcarle@quarkslab.com
Bruno Dorsemaine bruno.dorsemaine@orange.com
Fernand Lone-Sang flonesang@quarkslab.com
Alexandre Quint aquint@quarkslab.com

INNOVATIVE SECURITY

www.quarkslab.com

contact@quarkslab.com | @quarkslab