FireEye™

Protection contre les Attaques de Nouvelle Génération

Ou comment identifier et bloquer un événement Zéro

« L'Art de la guerre est basé sur la tromperie»

Sun Tzu, The Art of the War. Attitude of the Army

.

Yogi Chandiramani

Denis Gadonnet

NSS Labs

Product	Malware Blocking%	Exploit Blocking %	Performance Impact
Trend Micro	90.1%	19%	0.21
McAfee	85.2%	73%	0.67
F-Secure	80.4%	75%	1.17
Norman	77.2%	25%	0.05
Sunbelt	75.3%	3%	0.37
Microsoft	75.0%	60%	0.05
Panda	73.1%	10%	0.17
Symantec	72.3%	64%	0.09
Kaspersky	71.3%	75%	0.38
Eset	60.0%	44%	0.09
AVG	54.8%	15%	0.58

TABLE 1: PRODUCT GUIDANCE

OVERALL RESULTS & FINDINGS

- Malware protection is far from commodity, with effectiveness ranging between 54% and 90%, a 36% spread.
- Cybercriminals have between a 10% - 45% chance of getting past your AV with Web Malware (depending on the product).
- Cybercriminals have between 25% - 97% chance of compromising your machine using exploits (depending on the product).
- Expect use of exploits to increase since it is far more effective than traditional malware.

NSS Labs

CONSUMER ANTI-MALWARE PRODUCTS
GROUP TEST REPORT

FireEye

Pas une semaine.....

Norway Cyber Attack Tar
Systems

By Chloe Albanesius | November 18, 2011 01:44pm EST

De : ""Comission Nationale de lInformatique et des Libertés"" <CNIL@gmx.com>
À : [redacted]
Envoyé le : Lundi 23 juillet 2012 19h17
Objet : Dossier EV580007 Unige

CNIL

La Commission nationale de l'informatique et des libertés est chargée de veiller à ce l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité hu droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.
Elle exerce ses missions conformément à la loi informatique et libertés qui la qualifie administrative indépendante.

Bonjour,

Nous avons été informé par l'université de psychologie et des sciences de l'éducatio n'avez pas reçu votre rémunration. Après renseignement auprès de La Poste, il est que vous n'avez pas reçu votre envoie postal. Ceci est sûrement dû à une erreur d votre adresse de notre part, un changement d'adresse ou encore un problème lié à aux-lettres.

Veuillez ci-dessous saisire votre VERITABLE adresse ACTUELLE :

NOM *	
Prénom *	

Hackers wanted $50,000 to keep Symantec source ode private

As part of a sting operation, Symantec told a hacker group that it would pay $50,000 to keep the source code for eut coûter jusqu'à 300 000 dollars ...e Internet, the

Une filiale de Schneider Electric se fait dérober des informations

Le 27 septembre 2012 (13:30)

Une filiale du groupe français a averti ses clients - de grands noms de l'énergie - que son réseau avait été pénétré par des pirates. Ceux-ci sont parvenus à dérober des informations concernant des systèmes

pertes d'informations sensibles, notamment des biens de propriété intellectuelle et des secrets

Chine
Mar 9, 2011 | 2

Tweet

SHARE

Libération

Nex

Dernière r

Recherc

ACTUALITÉS | DÉBATS | CULTURE

A la Une | Éditos | Politiques | Société

Chinese hacke
as part of the l

POLITIQ

RSA br
stolen

L'Ely
cybe

La cyberdéfense : un enjeu mondial, une priorité nationale

Rapport d'information de M. Jean-Marie BOCKEL, fait au nom de la commission des affaires étrangères, de la défense et des forces armées
n° 681 (2011-2012) - 18 juillet 2012

Breach, 200K

Rue89 | Le nouvel Observat

LES RUBRIQUES | Plus de mariage | Arnault en Belgique

VIRUS 24/08/201

Cyberattaque contre l'une des p importantes compagnies pétrolières

Sid Ahmed Hammouche | Journaliste de La Liberté

laliberte.ch

(les champs marqués d'un * sont obligatoires)

Vous recevrez votre paiement en espèce, conformément au contrat établit avec l'Université de Psychologie de Genève.

Ce paiement aura lieu avant le 2 septembre 2012.

Pour en savoir davantage sur vos droits, rendez-vous sur le site :

Legifrance.gouv.fr
LE SERVICE PUBLIC DE LA DIFFUSION DU DROIT

choisie par les attaquants et opérateurs du boti présente plusieurs avantages, mais aussi certai inconvénients », comme ils l'ont écrit dans un blog. Pour ce qui est des avantages, le serveur de commande et de tre bloqué par des chercheurs ou des autorités, car il n'est pas tion réelle.

...ologies

...laytime | Libertés numériques | Téléphonie mobile | Dro

de dollars détournés berattaque visant des

Le Monde.fr avec AFP | 26.06.2012 à 22h32 • Mis à jour le 27.06.2012 à 08h51

Photo: Jason Allen

Source code belonging to VMWare has leaked to the internet after apparently being stolen by a hacker who claims to have obtained it from a Chinese firm's network.

FireEye™

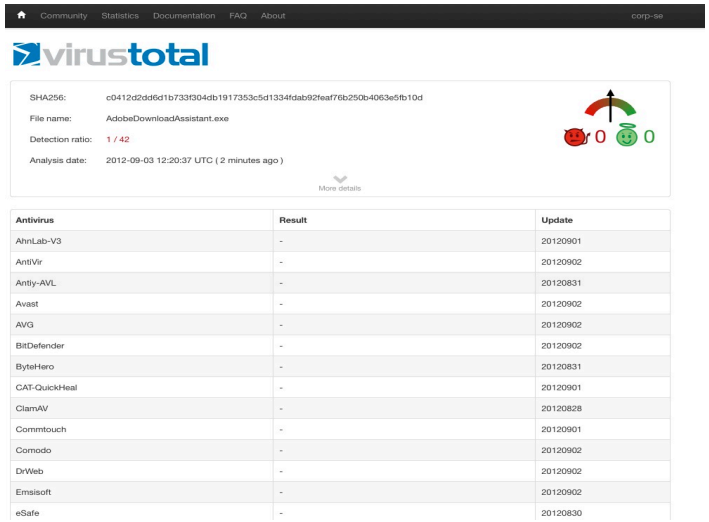
L'art suprême de la guerre est de soumettre l'ennemi sans combattre

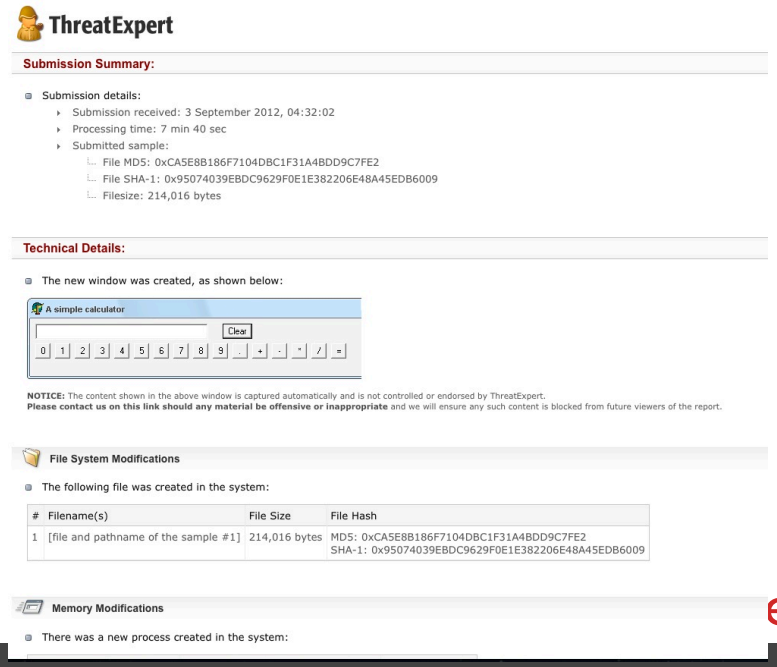
Sun Tzu, The Art of the War. Offensive strategy.

Les Cybercriminels ont accès aux mêmes outils

- Notre méthodologie sécurité repose sur une approche collaborative
  - ✓ Partage efficace d'information
  - X Cybercriminels ont accès aux mêmes données

"It's not a fair war between the attackers and the defenders when the attackers have access to our weapons." (Mikko Hypponen, CTO F-Secure)





eEye™

Complexité des logiciels

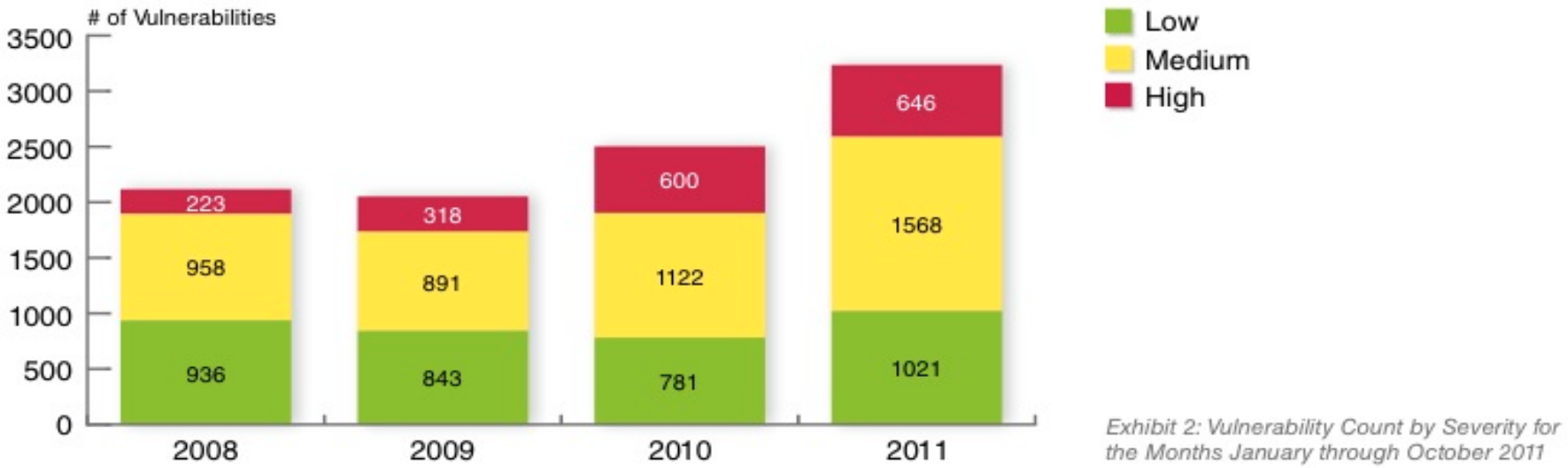
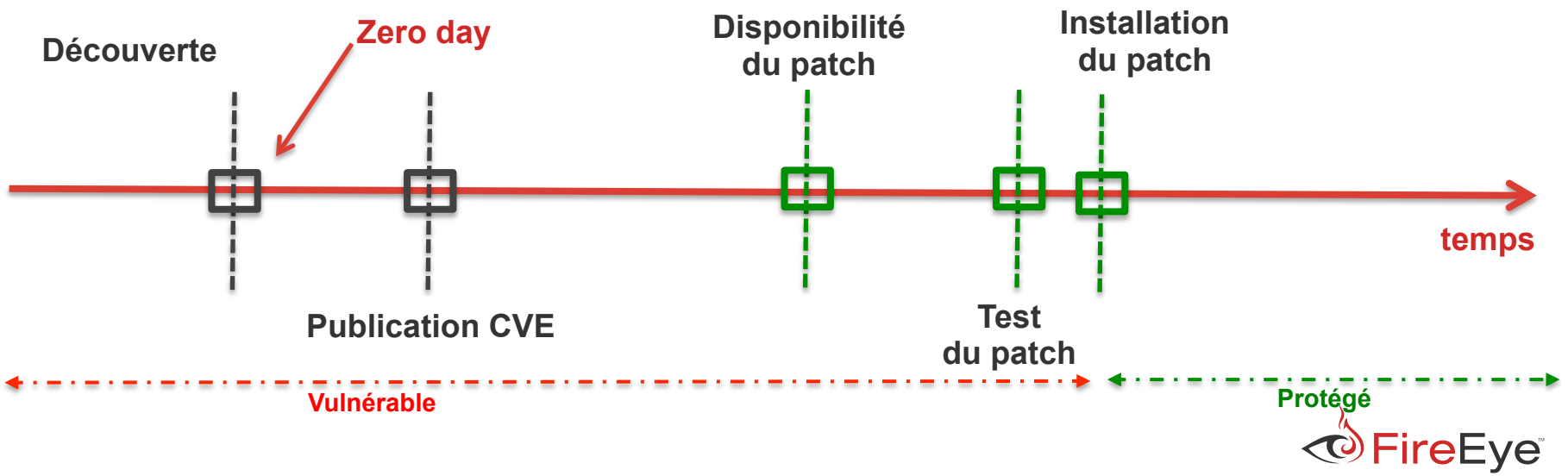


Exhibit 2: Vulnerability Count by Severity for the Months January through October 2011



FireEye

Les cybercriminels s'adaptent …

- Dès que des contre mesures sont déployées par les outils de sécurité, de nouvelles techniques pour les contourner sont utilisées par les cybercriminels;
  - Code Polymorphic
  - Binaire compilé à la volée en fonction du navigateur du client et l'adresse IP du client pour une infection optimum
  - Domaines "jetables"
  - Malwares sur mobile pour fraudes financières
  - Modèle P2P pour infrastrcutures CnC
  - Malwares qui s'autodétruisent
  - …

FireEye

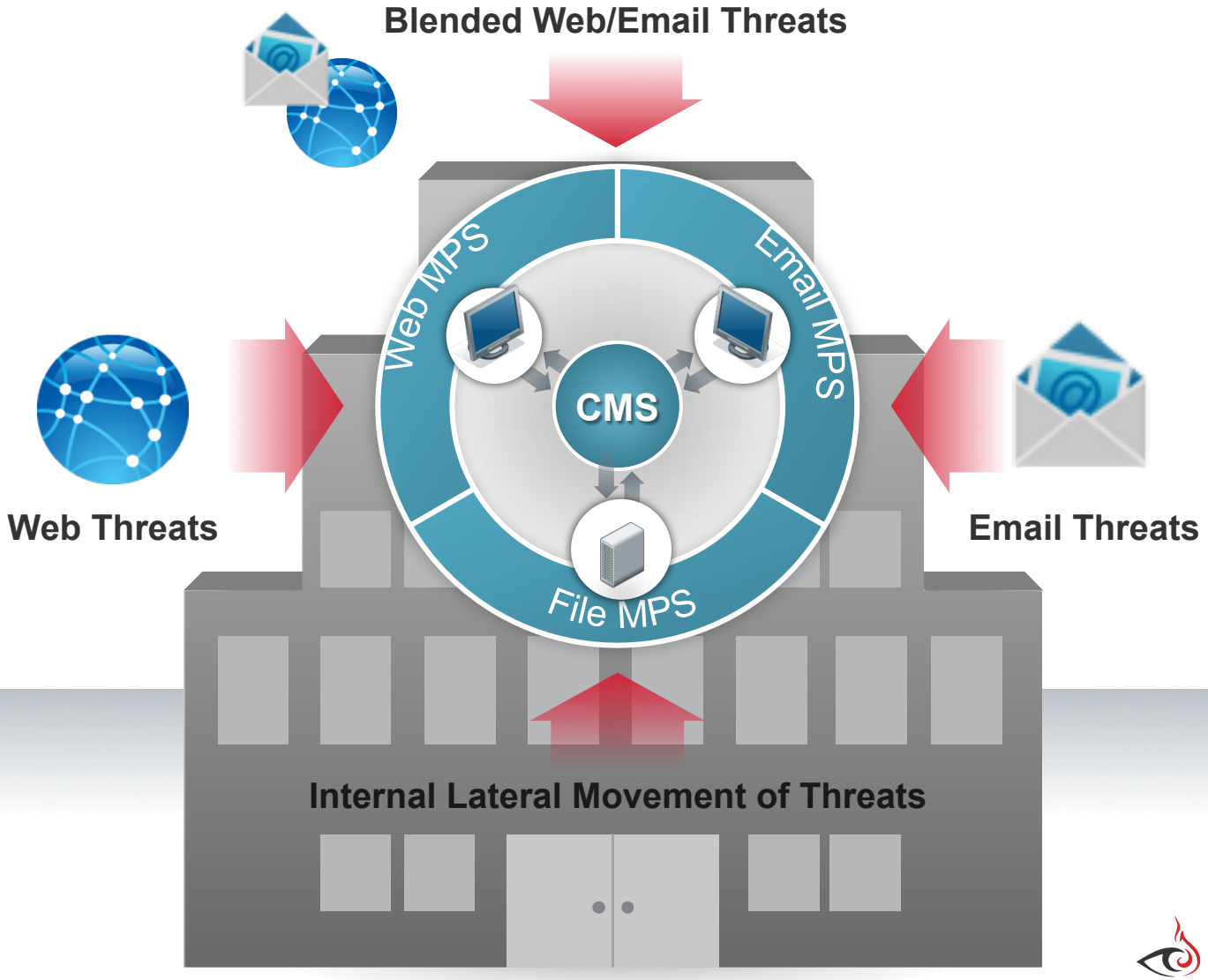
FireEye™

La Réponse FireEye

« L'Art de la guerre est basé sur la tromperie»

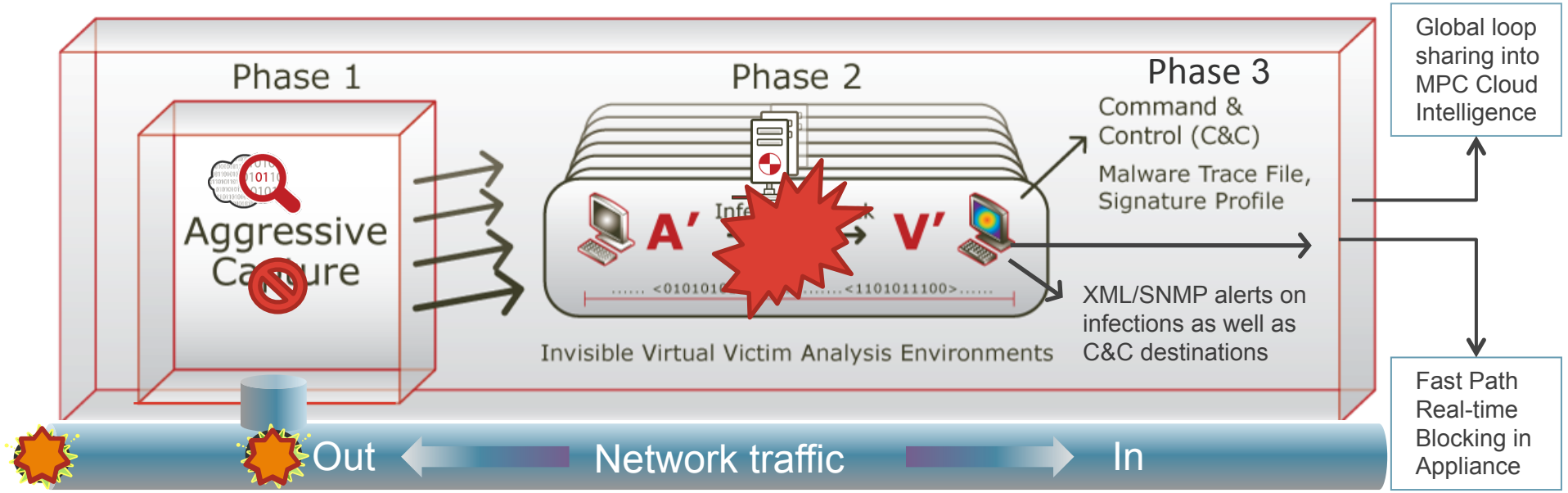
Sun Tzu, The Art of the War.

Protection Multi-Vecteur



FireEye

Identification des attaques de type Zero-Day



Phase 1: Capture Aggressive utilisant des techniques d'heuristiques et de signatures

- Déploiement out-of-band/passive (SPAN/TAP)
- Capture multi protocolaire HTML, fichiers (e.g. PDF), & EXEs

Phase 2: Analyse dans une machien virtuelle

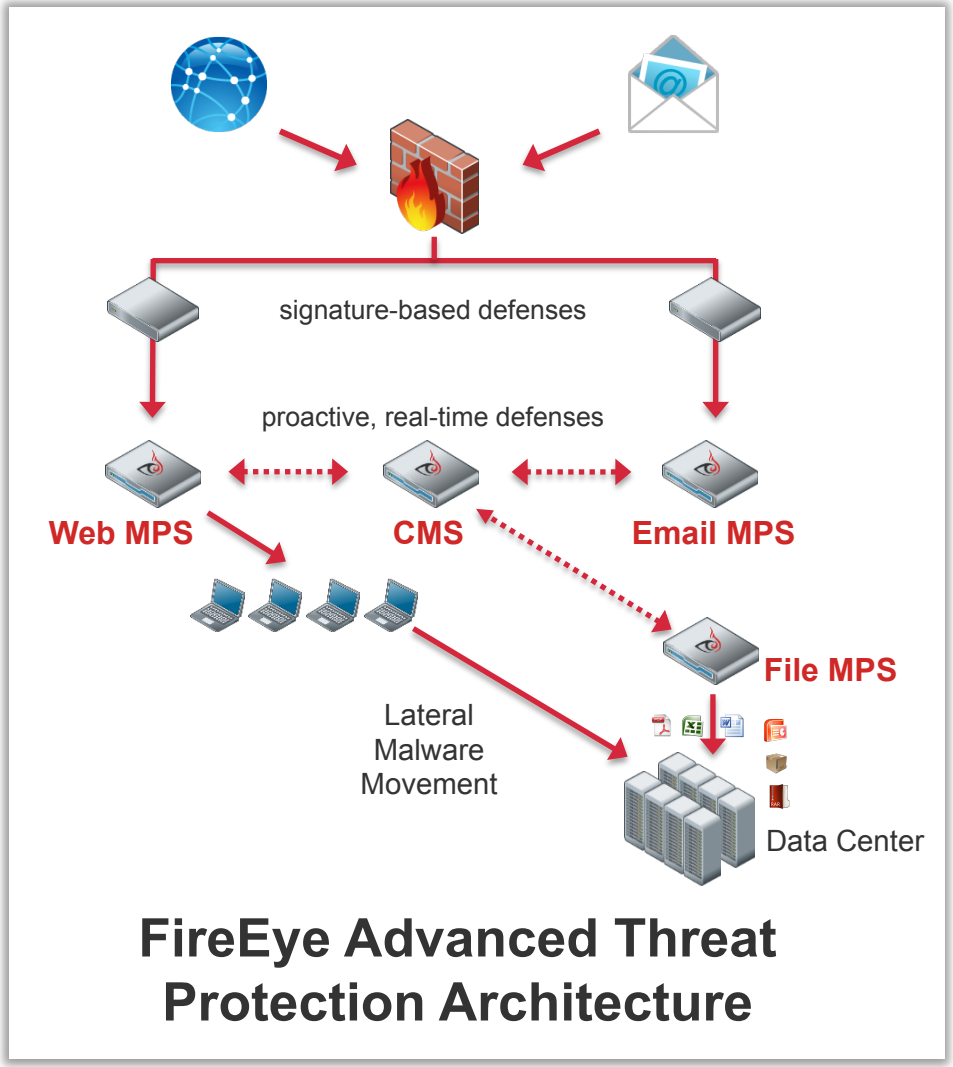
- Identification des comportements malicieux
- Minimum de false positive

Phase 3: Filtrage des callback

- Les informations sensibles ne sont pas dérobées

FireEye

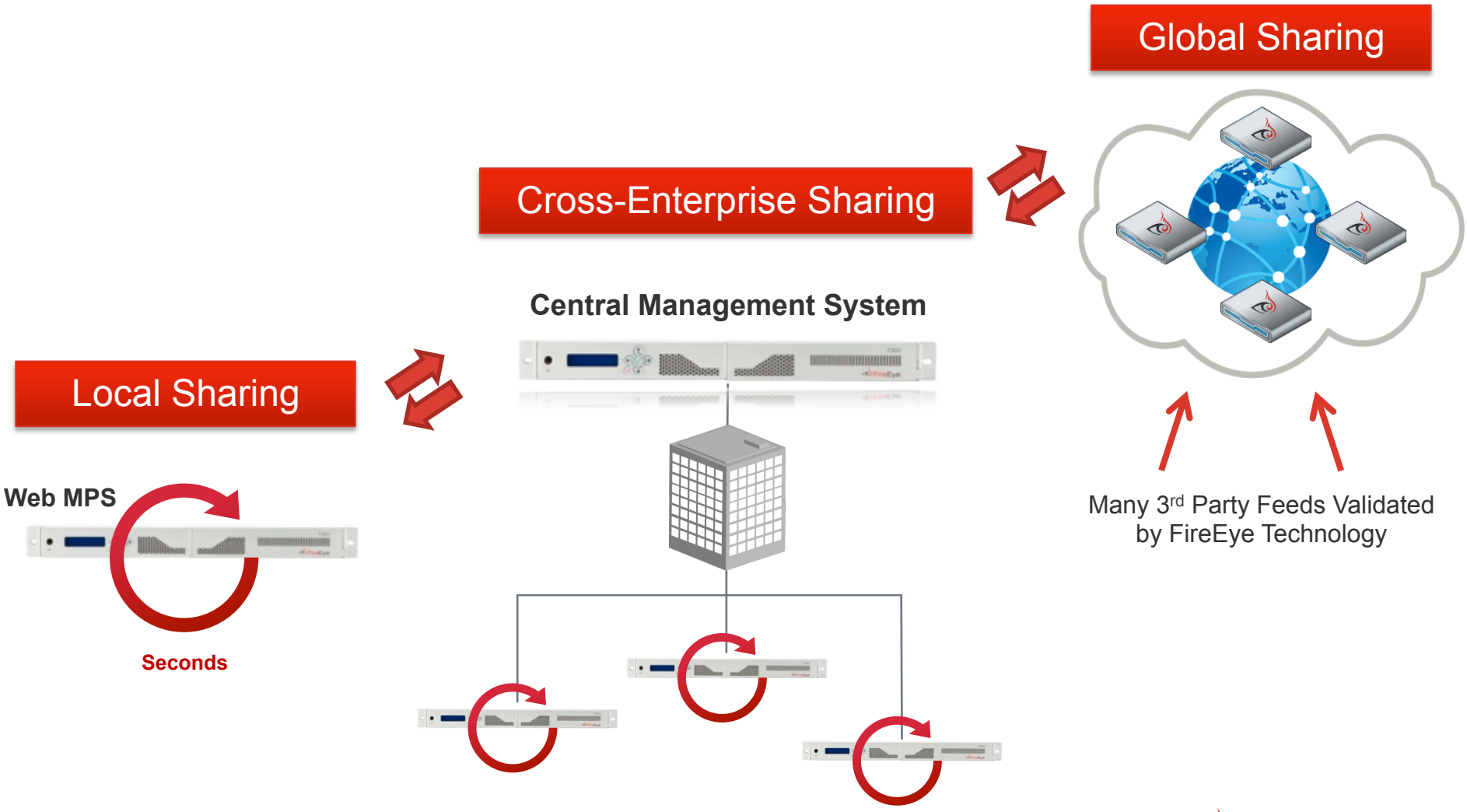
Filtrage temps réel



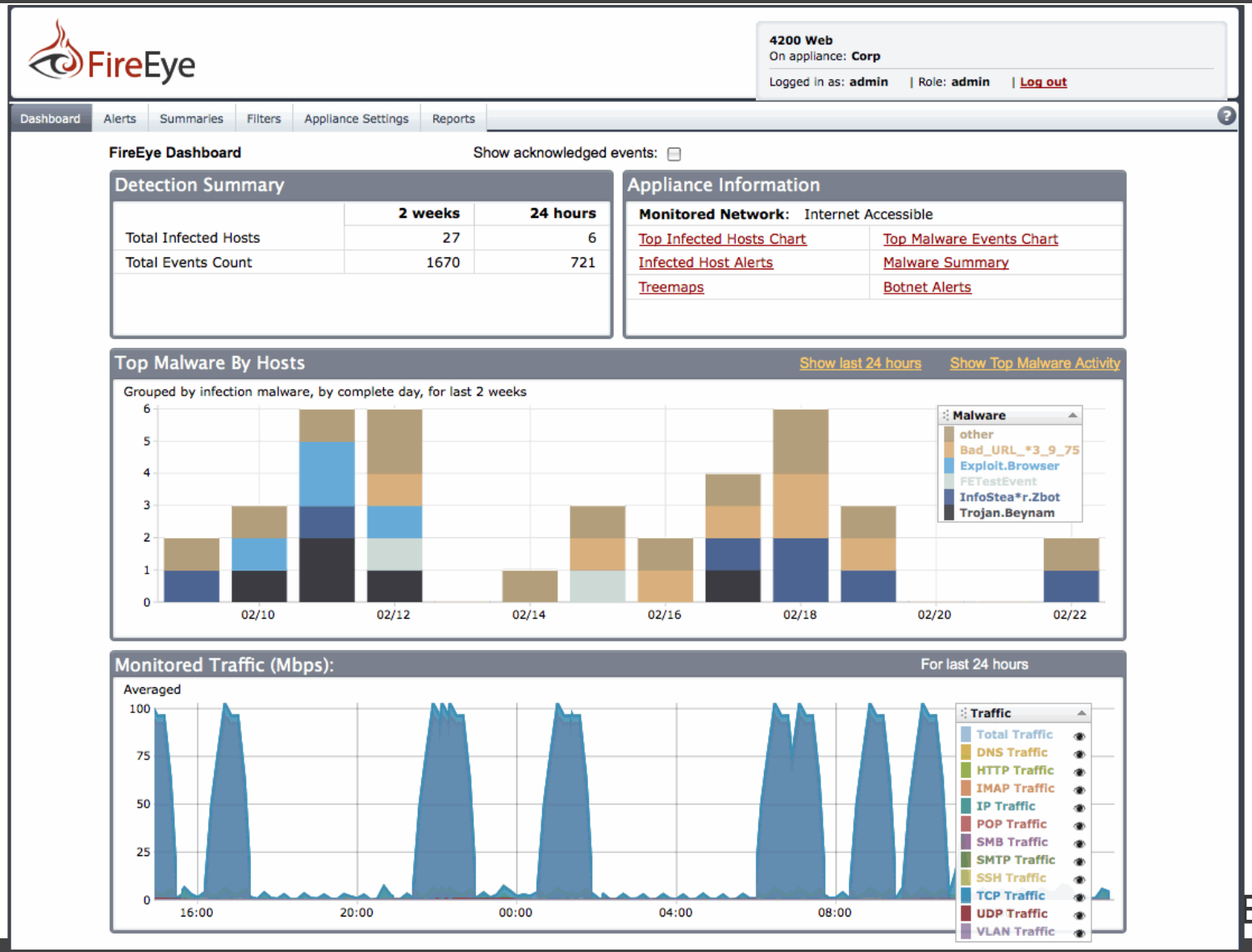
- Filtrage sur tous les produits Fireeye
  - Filtrage des attaques web zero-day
  - Filtrage multi-protocolaire des callbacks
  - Attachements zero-day mis en quarantaine
  - Fichiers zero-day mis en quarantaine
- Rapport détaillé permettant de prendre des actions lorsqu'un évènement malicieux est identifié

FireEye

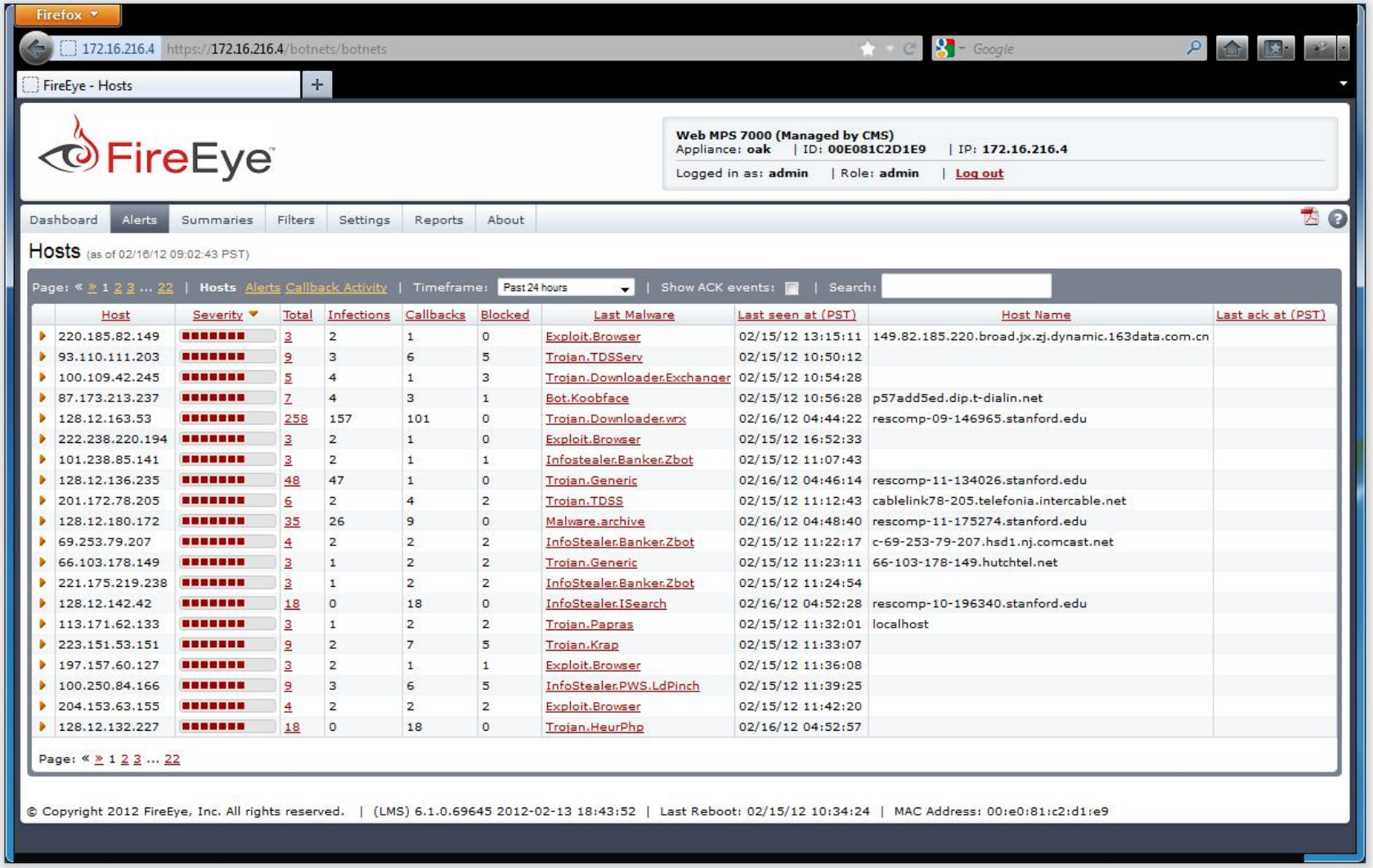
Partage Global des Profils d'Attaques



Dashboard – Malware Protection Status

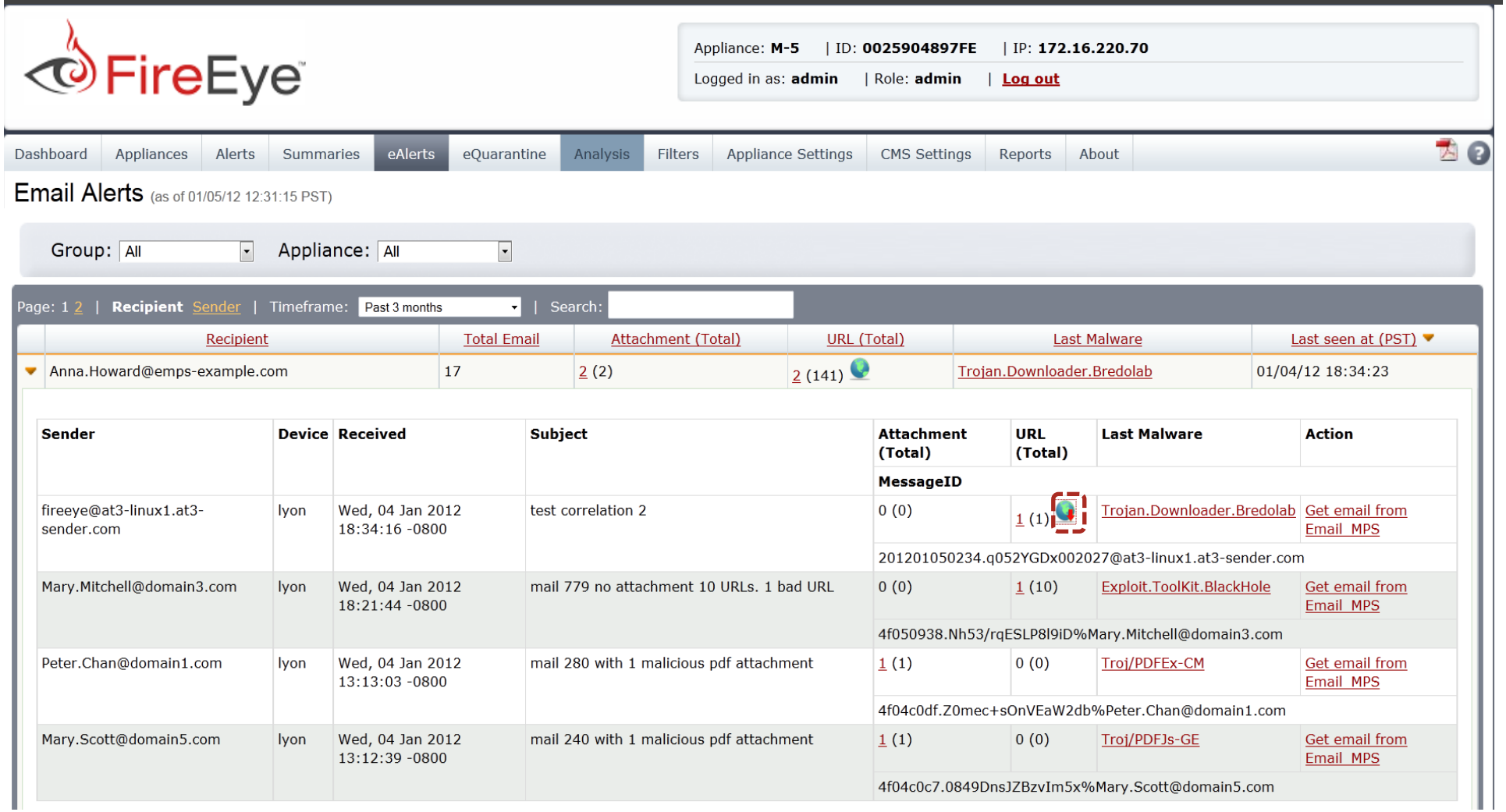


Activité Malware



FireEye

Correlation des attaques



FireEye

Appliance: **M-5** | ID: **0025904897FE** | IP: **172.16.220.70**

Logged in as: **admin** | Role: **admin** | **Log out**

Dashboard | Appliances | Alerts | Summaries | eAlerts | eQuarantine | Analysis | Filters | Appliance Settings | CMS Settings | Reports | About

Email Alerts (as of 01/05/12 12:31:15 PST)

Group: All Appliance: All

Page: 1 2 | **Recipient** Sender | Timeframe: Past 3 months | Search:

Recipient	Total Email	Attachment (Total)	URL (Total)	Last Malware	Last seen at (PST)
Anna.Howard@emps-example.com	17	2 (2)	2 (141)	Trojan.Downloader.Bredolab	01/04/12 18:34:23

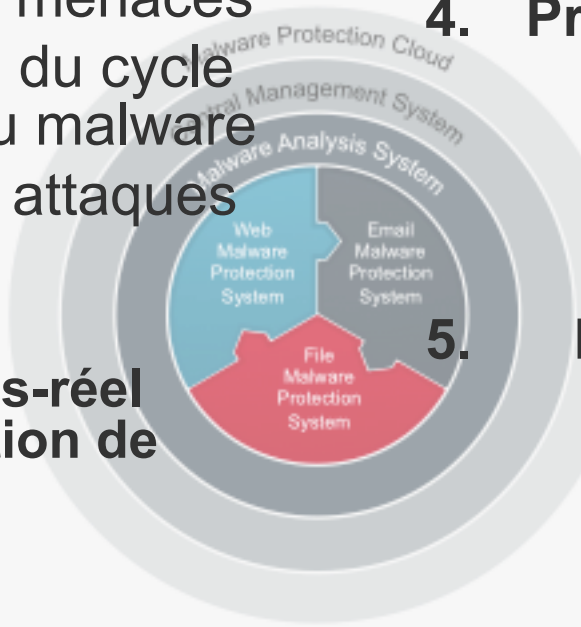
Sender	Device	Received	Subject	Attachment (Total)	URL (Total)	Last Malware	Action
				MessageID			
fireeye@at3-linux1.at3-sender.com	lyon	Wed, 04 Jan 2012 18:34:16 -0800	test correlation 2	0 (0)	1 (1)	Trojan.Downloader.Bredolab	Get email from Email_MPS
				201201050234.q052YGDx002027@at3-linux1.at3-sender.com			
Mary.Mitchell@domain3.com	lyon	Wed, 04 Jan 2012 18:21:44 -0800	mail 779 no attachment 10 URLs. 1 bad URL	0 (0)	1 (10)	Exploit.ToolKit.BlackHole	Get email from Email_MPS
				4f050938.Nh53/rqESLP8l9iD%Mary.Mitchell@domain3.com			
Peter.Chan@domain1.com	lyon	Wed, 04 Jan 2012 13:13:03 -0800	mail 280 with 1 malicious pdf attachment	1 (1)	0 (0)	Troj/PDFEx-CM	Get email from Email_MPS
				4f04c0df.Z0mec+sOnVEaW2db%Peter.Chan@domain1.com			
Mary.Scott@domain5.com	lyon	Wed, 04 Jan 2012 13:12:39 -0800	mail 240 with 1 malicious pdf attachment	1 (1)	0 (0)	Troj/PDFJs-GE	Get email from Email_MPS
				4f04c0c7.0849DnsJZBzvIm5x%Mary.Scott@domain5.com			

FireEye

En Résumé

1. **Défense Dynamique et Multi-Vecteurs**
   - Analyse en temps réel des VRAIES menaces
   - Identification du cycle d'infection du malware
   - Blocage des attaques avancées

2. **Protection temps-réel contre l'exfiltration de données**



3. **Minimum de Faux Positives**

4. **Protection 360°**
   - BYOD
   - Clefs USB, Data Centers

5. **ROI Elevé**

"FireEye me permet en 15 minutes d'identifier et de bloquer une attaque Zéro Day et call back qui me prend en général de 1h à 24h"
Directeur SOC – France

FireEye

FireEye™

Don’t trust us, Test us

MERCI

Retrouvez-nous sur le Stand 7

www.FireEye.com

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce