



# 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.



CONSUMER ANTI-MALWARE PRODUCTS  
GROUP TEST REPORT



# Pas une semaine.....

## Norway Cyber Attack Targets Systems



By **Chloe Albanesius**

November 18, 2011 01:44pm EST

### Chine

Mar 9, 2011 | 2



SHARE



Nex

Dernière r

Recherch

■ ACTUALITÉS ■ DÉBATS ■ CULTURE

A la Une | Édits | Politiques | Société



POLITIQU

## La cyberdéfense : un enjeu mondial, une priorité nationale

RSA bi  
stolen

L'Ely  
cybe

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

Arnaut en Belgique

VIRUS

24/08/2011

## Cyberattaque contre l'une des plus importantes compagnies pétrolières

Sid Ahmed Hammouche | Journaliste de La Liberté

laliberte.ch

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



La Commission nationale de l'informatique et des libertés est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux 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 d'organisme administratif indépendant.

Bonjour,

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

Veillez ci-dessous saisir votre VÉRITABLE adresse ACTUELLE :

NOM *	
Prénom *	

## Hackers wanted \$50,000 to keep Symantec source code private

As part of a sting operation, Symantec told a hacker group that it would pay \$50,000 to keep the source code for its Internet, the

peut coûter jusqu'à 300 000 dollars

## 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

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

## Logies

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.



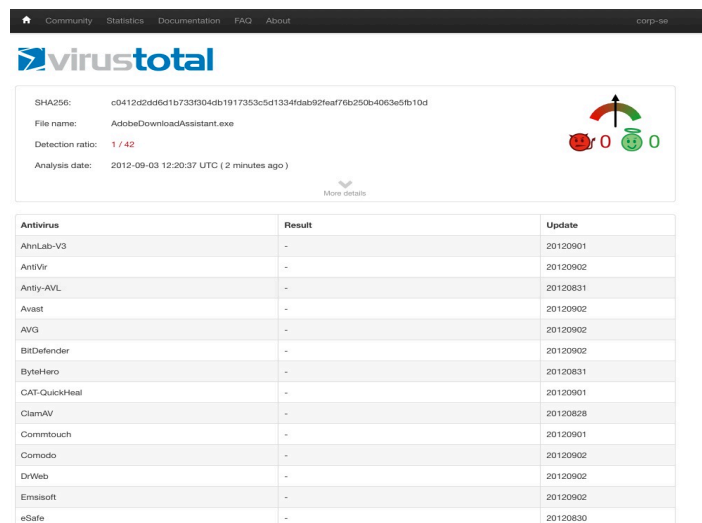
L'art suprême de la guerre est de  
soumettre l'ennemi sans combattre

*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)*

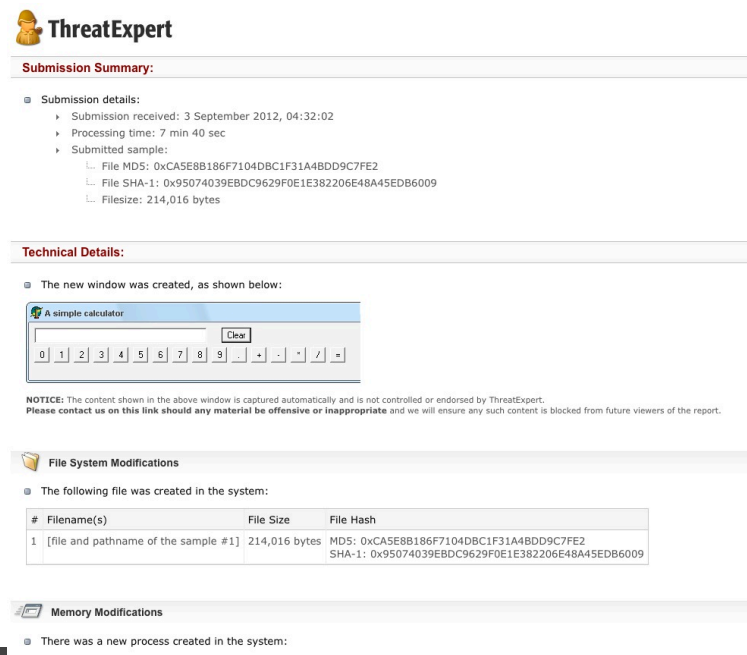


Community Statistics Documentation FAQ About corp-se

**virustotal**

SHA256: c0412d2d56d1b733f04db1917353c5d1334f4ab92feaf76b250b4063e5b10d  
File name: AdobeDownloadAssistant.exe  
Detection ratio: 1 / 42  
Analysis date: 2012-09-03 12:20:37 UTC ( 2 minutes ago )

Antivirus	Result	Update
AhnLab-V3	-	20120901
AntiVir	-	20120902
Antiy-AVL	-	20120831
Avast	-	20120902
AVG	-	20120902
BitDefender	-	20120902
ByteHero	-	20120831
CAT-QuickHeal	-	20120901
ClamAV	-	20120828
CommTouch	-	20120901
Comodo	-	20120902
DrWeb	-	20120902
Emsisoft	-	20120902
eSafe	-	20120830

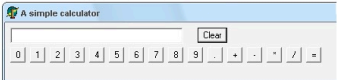


**ThreatExpert**

**Submission Summary:**

- Submission details:
  - Submission received: 3 September 2012, 04:32:02
  - Processing time: 7 min 40 sec
  - Submitted sample:
    - File MD5: 0xCASE8B186F7104DBC1F31A4BDD9C7FE2
    - File SHA-1: 0x95074039EBDC9629F0E1E382206E48A45EDB6009
    - Filesize: 214,016 bytes

**Technical Details:**

- The new window was created, as shown below:  


NOTICE: The content shown in the above window is captured automatically and is not controlled or endorsed by ThreatExpert. Please contact us on this link should any material be offensive or inappropriate and we will ensure any such content is blocked from future viewers of the report.

**File System Modifications**

- The following file was created in the system:

#	Filename(s)	File Size	File Hash
1	[file and pathname of the sample #1]	214,016 bytes	MD5: 0xCASE8B186F7104DBC1F31A4BDD9C7FE2 SHA-1: 0x95074039EBDC9629F0E1E382206E48A45EDB6009

**Memory Modifications**

- There was a new process created in the system:

# Complexité des logiciels

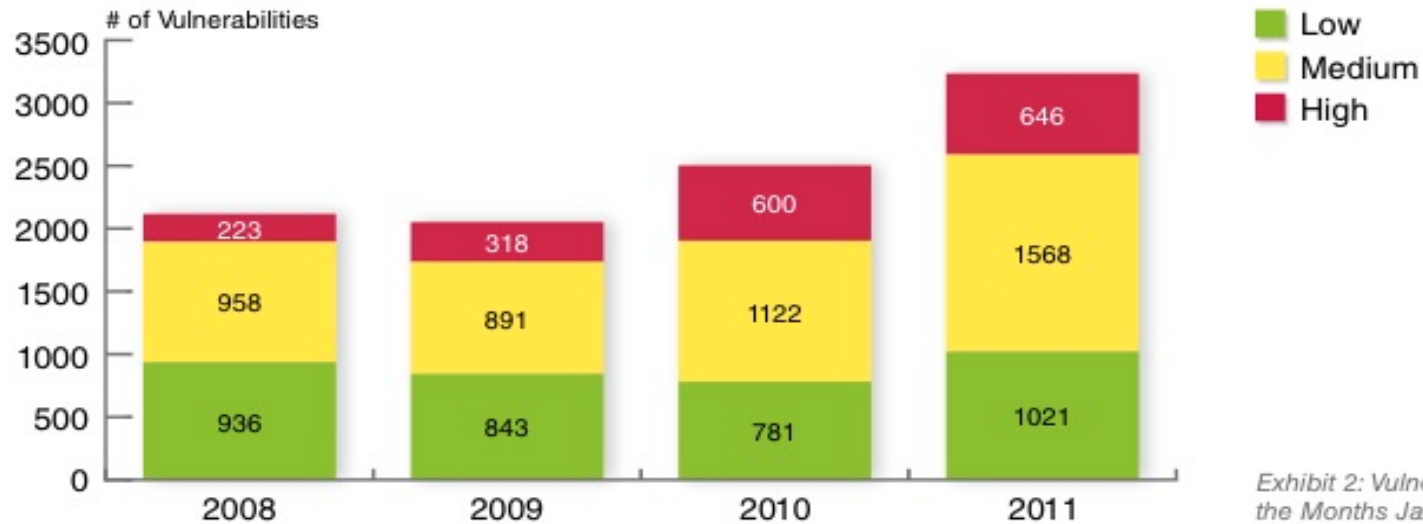
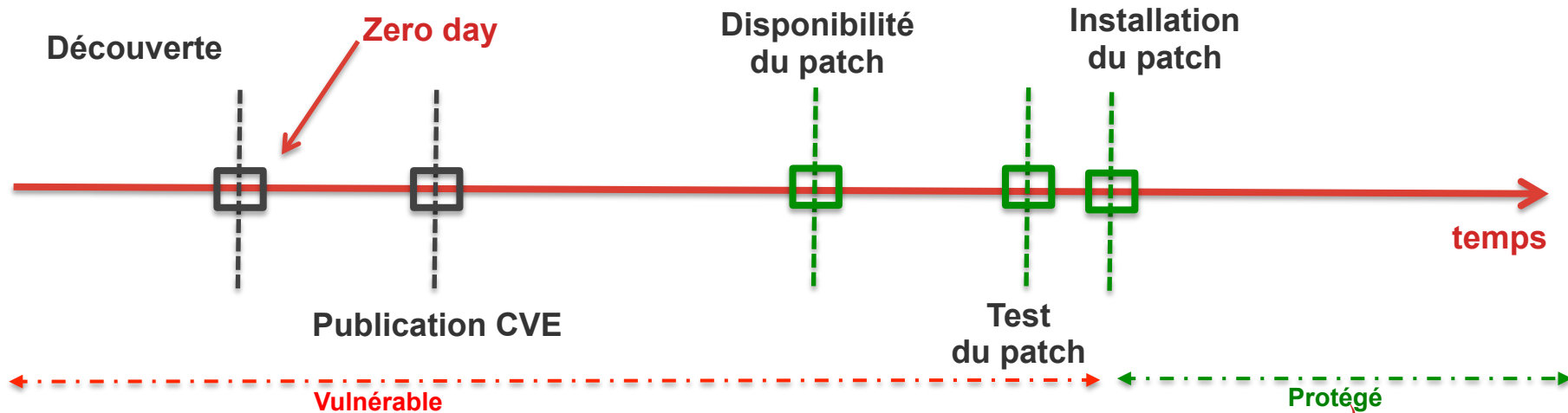


Exhibit 2: Vulnerability Count by Severity for the Months January through October 2011



# 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 infrastructures CnC
  - Malwares qui s'autodétruisent
  - ...





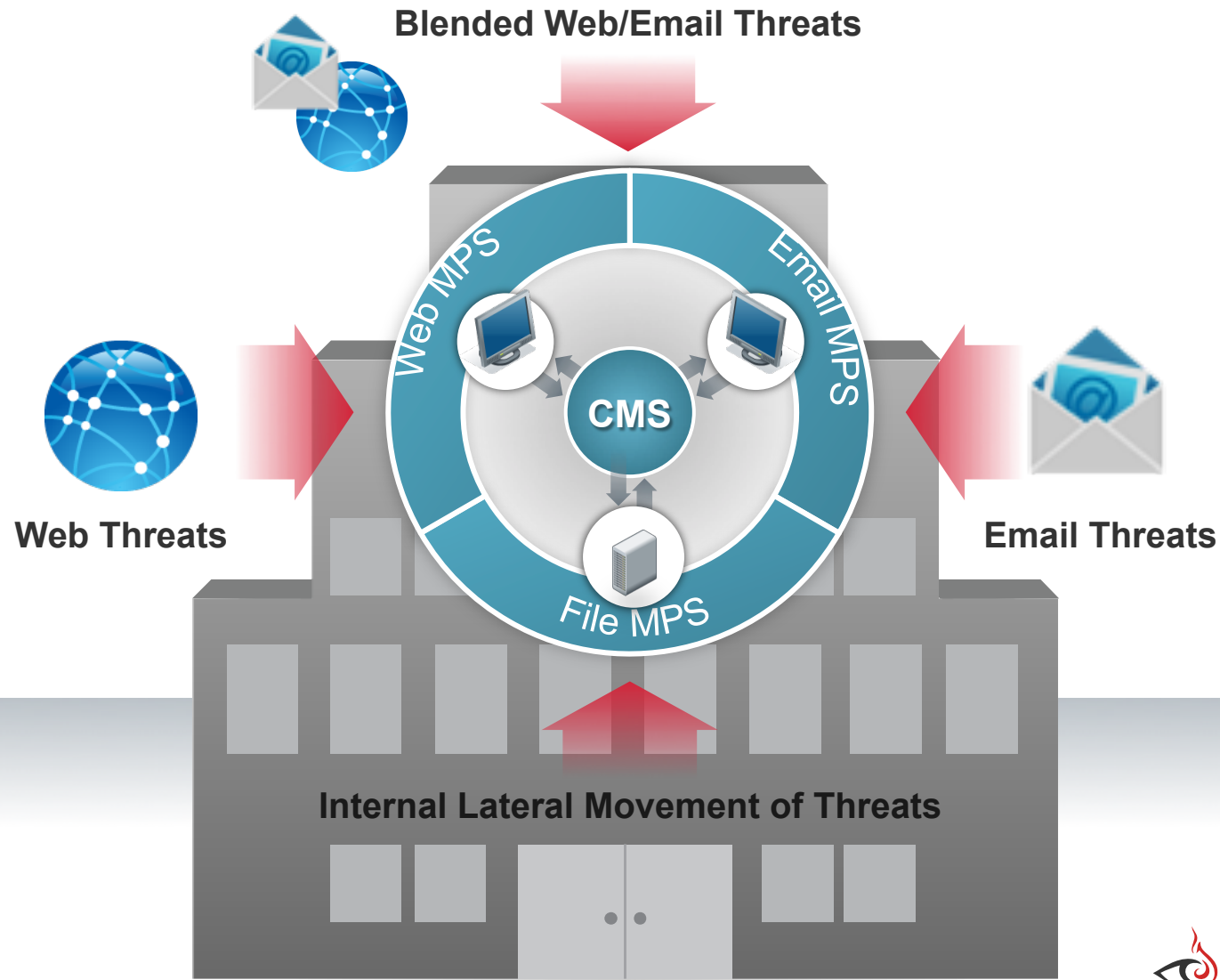
# La Réponse FireEye

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

*Sun Tzu, The Art of the War.*



# Protection Multi-Vecteur



# 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 machine virtuelle

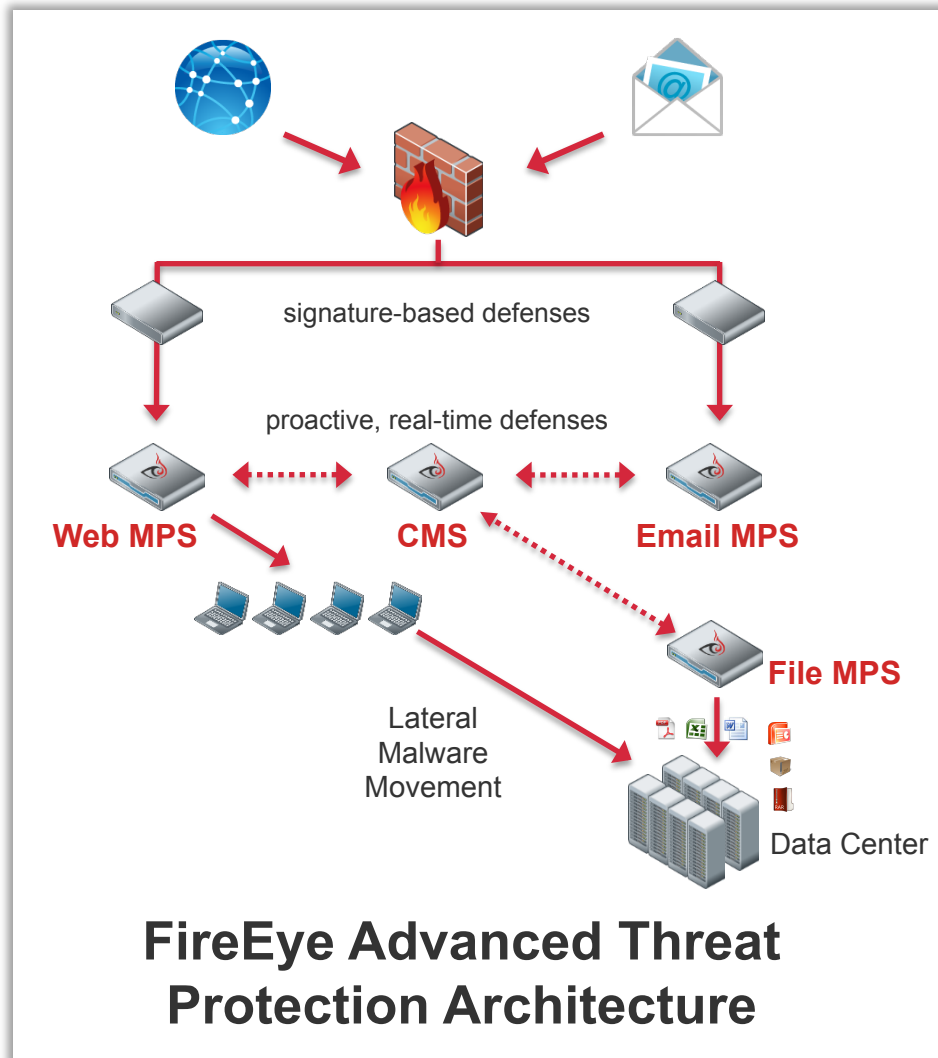
- Identification des comportements malicieux
- Minimum de false positive

Phase 3: Filtrage des callback

- Les informations sensibles ne sont pas dérobées

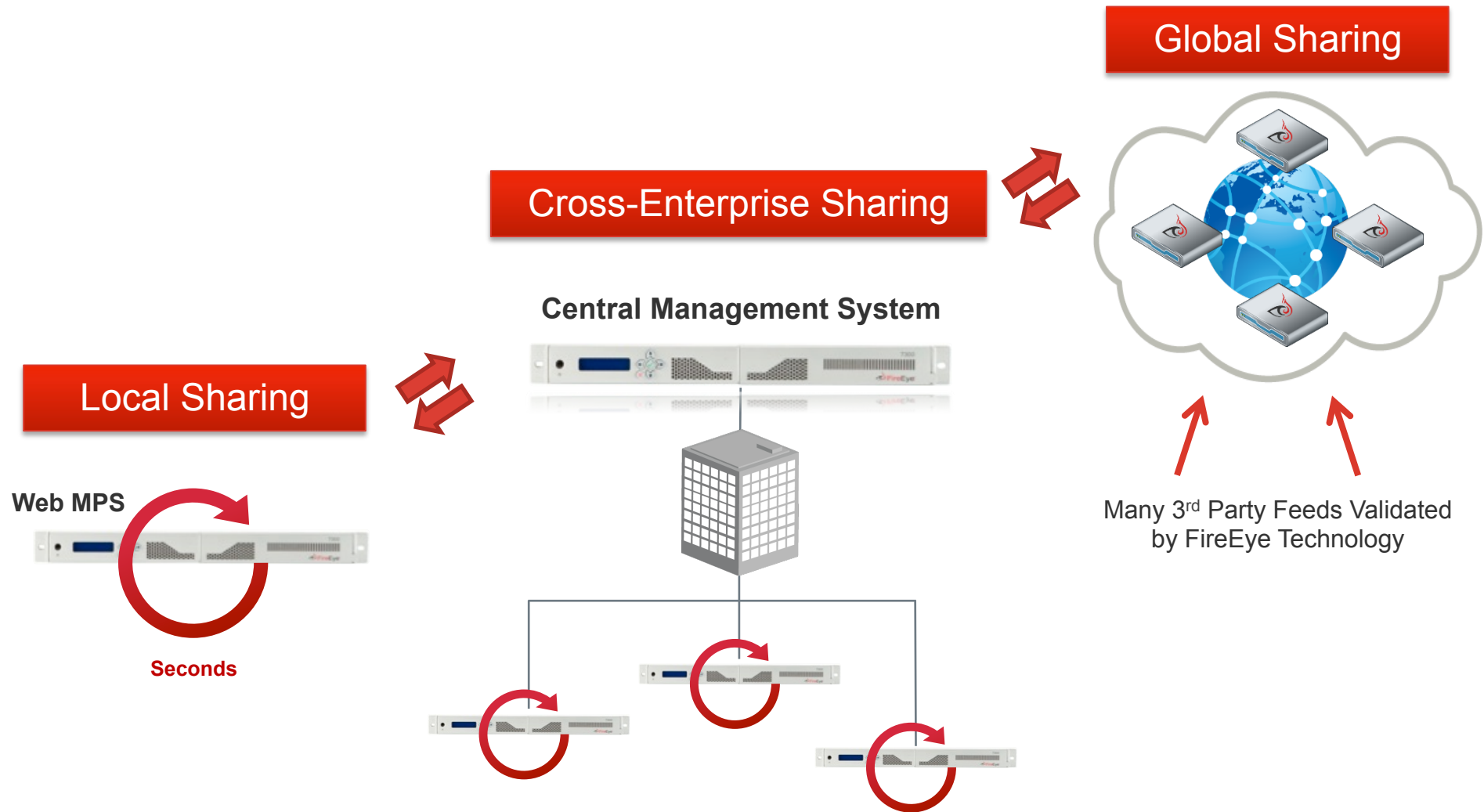


# Filtrage temps réel

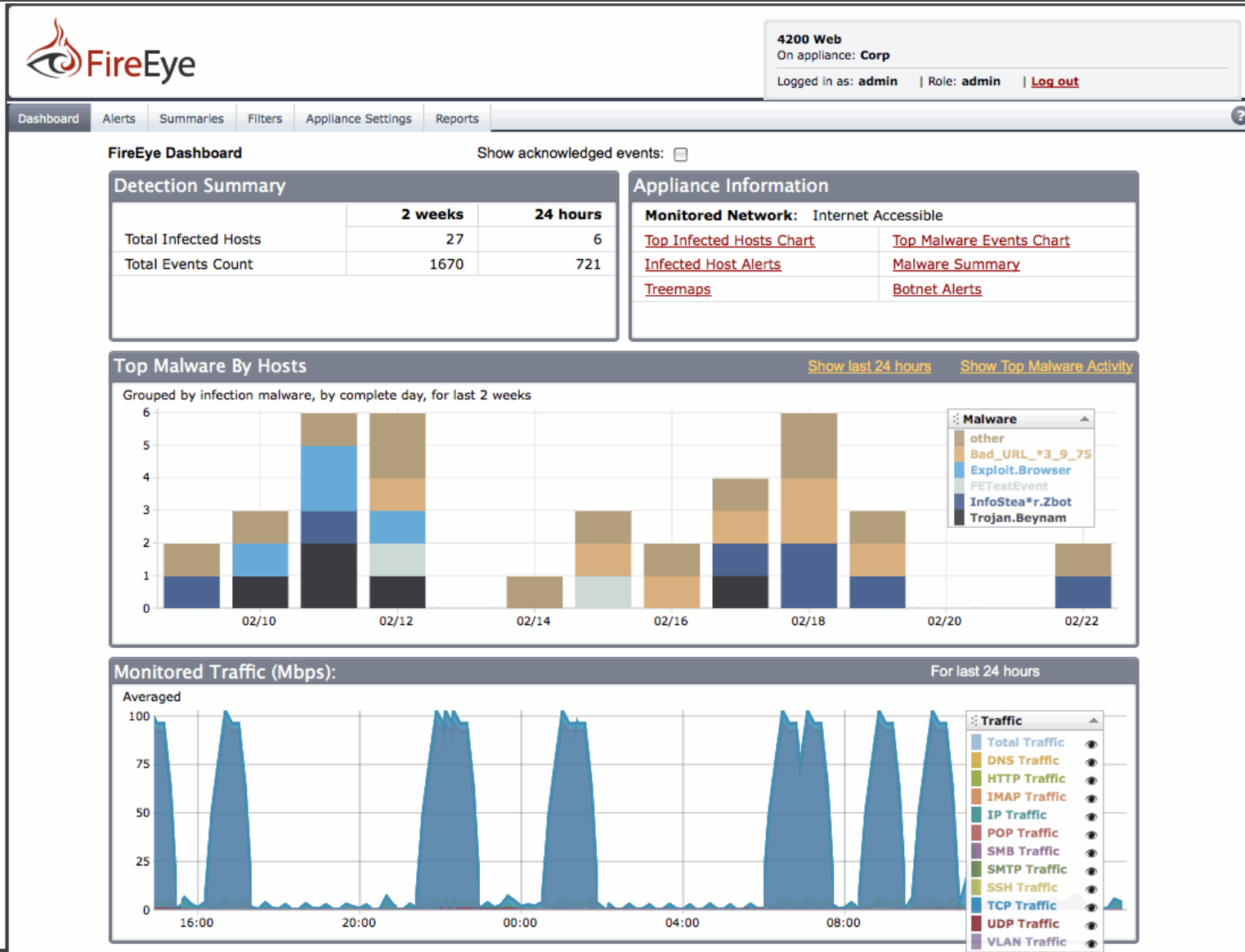


- Filtrage sur tous les produits Fireeye
  - Filtrage des attaques web zero-day
  - Filtrage multi-protocolaire des callbacks
  - Attachements zero-day mis en quarantaine
  - Fichiers zero-day mis en quarantaine
- Rapport détaillé permettant de prendre des actions lorsqu'un évènement malicieux est identifié

# Partage Global des Profils d'Attaques



# Dashboard – Malware Protection Status



# Activité Malware

Firefox | 172.16.216.4 | https://172.16.216.4/botnets/botnets | Google

FireEye - Hosts

**FireEye**

Web MPS 7000 (Managed by CMS)  
Appliance: oak | ID: 00E081C2D1E9 | IP: 172.16.216.4  
Logged in as: admin | Role: admin | [Log out](#)

Dashboard Alerts Summaries Filters Settings Reports About

**Hosts** (as of 02/16/12 09:02:43 PST)

Page: << 1 2 3 ... 22 | Hosts Alerts Callback Activity | Timeframe: Past 24 hours | Show ACK events:  | Search:

Host	Severity	Total	Infections	Callbacks	Blocked	Last Malware	Last seen at (PST)	Host Name	Last ack at (PST)
220.185.82.149	3	2	1	0	Exploit.Browser	02/15/12 13:15:11	149.82.185.220.broad.jx.zj.dynamic.163data.com.cn		
93.110.111.203	9	3	6	5	Trojan.TDSServ	02/15/12 10:50:12			
100.109.42.245	5	4	1	3	Trojan.Downloader.Exchanger	02/15/12 10:54:28			
87.173.213.237	7	4	3	1	Bot.Koobface	02/15/12 10:56:28	p57add5ed.dip.t-dialin.net		
128.12.163.53	258	157	101	0	Trojan.Downloader.wrx	02/16/12 04:44:22	rescomp-09-146965.stanford.edu		
222.238.220.194	3	2	1	0	Exploit.Browser	02/15/12 16:52:33			
101.238.85.141	3	2	1	1	InfoStealer.Banker.Zbot	02/15/12 11:07:43			
128.12.136.235	48	47	1	0	Trojan.Generic	02/16/12 04:46:14	rescomp-11-134026.stanford.edu		
201.172.78.205	6	2	4	2	Trojan.TDSS	02/15/12 11:12:43	cablelink78-205.telefonia.intercable.net		
128.12.180.172	35	26	9	0	Malware.archive	02/16/12 04:48:40	rescomp-11-175274.stanford.edu		
69.253.79.207	4	2	2	2	InfoStealer.Banker.Zbot	02/15/12 11:22:17	c-69-253-79-207.hsd1.nj.comcast.net		
66.103.178.149	3	1	2	2	Trojan.Generic	02/15/12 11:23:11	66-103-178-149.hutchtel.net		
221.175.219.238	3	1	2	2	InfoStealer.Banker.Zbot	02/15/12 11:24:54			
128.12.142.42	18	0	18	0	InfoStealer.ISearch	02/16/12 04:52:28	rescomp-10-196340.stanford.edu		
113.171.62.133	3	1	2	2	Trojan.Papras	02/15/12 11:32:01	localhost		
223.151.53.151	9	2	7	5	Trojan.Krap	02/15/12 11:33:07			
197.157.60.127	3	2	1	1	Exploit.Browser	02/15/12 11:36:08			
100.250.84.166	9	3	6	5	InfoStealer.PWS.LdPinch	02/15/12 11:39:25			
204.153.63.155	4	2	2	2	Exploit.Browser	02/15/12 11:42:20			
128.12.132.227	18	0	18	0	Trojan.HeurPhp	02/16/12 04:52:57			

Page: << 1 2 3 ... 22

© Copyright 2012 FireEye, Inc. All rights reserved. | (LMS) 6.1.0.69645 2012-02-13 18:43:52 | Last Reboot: 02/15/12 10:34:24 | MAC Address: 00:e0:81:c2:d1:e9



# Correlation des attaques



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:  Appliance:

Page: [1](#) [2](#) | Recipient [Sender](#) | Timeframe:  | Search:

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

Sender	Device	Received	Subject	Attachment (Total)	URL (Total)	Last Malware	Action
fireeye@at3-linux1.at3-sender.com	lyon	Wed, 04 Jan 2012 18:34:16 -0800	test correlation 2	0 (0)	<a href="#">1</a> (1)	<a href="#">Trojan.Downloader.Bredolab</a>	<a href="#">Get email from Email MPS</a>
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)	<a href="#">1</a> (10)	<a href="#">Exploit.ToolKit.BlackHole</a>	<a href="#">Get email from Email MPS</a>
4f050938.Nh53/rqESLP8I9ID%Mary.Mitchell@domain3.com							
Peter.Chan@domain1.com	lyon	Wed, 04 Jan 2012 13:13:03 -0800	mail 280 with 1 malicious pdf attachment	<a href="#">1</a> (1)	0 (0)	<a href="#">Troj/PDFEx-CM</a>	<a href="#">Get email from Email MPS</a>
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	<a href="#">1</a> (1)	0 (0)	<a href="#">Troj/PDFJs-GE</a>	<a href="#">Get email from Email MPS</a>
4f04c0c7.0849DnsJZBzvIm5x%Mary.Scott@domain5.com							



# 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

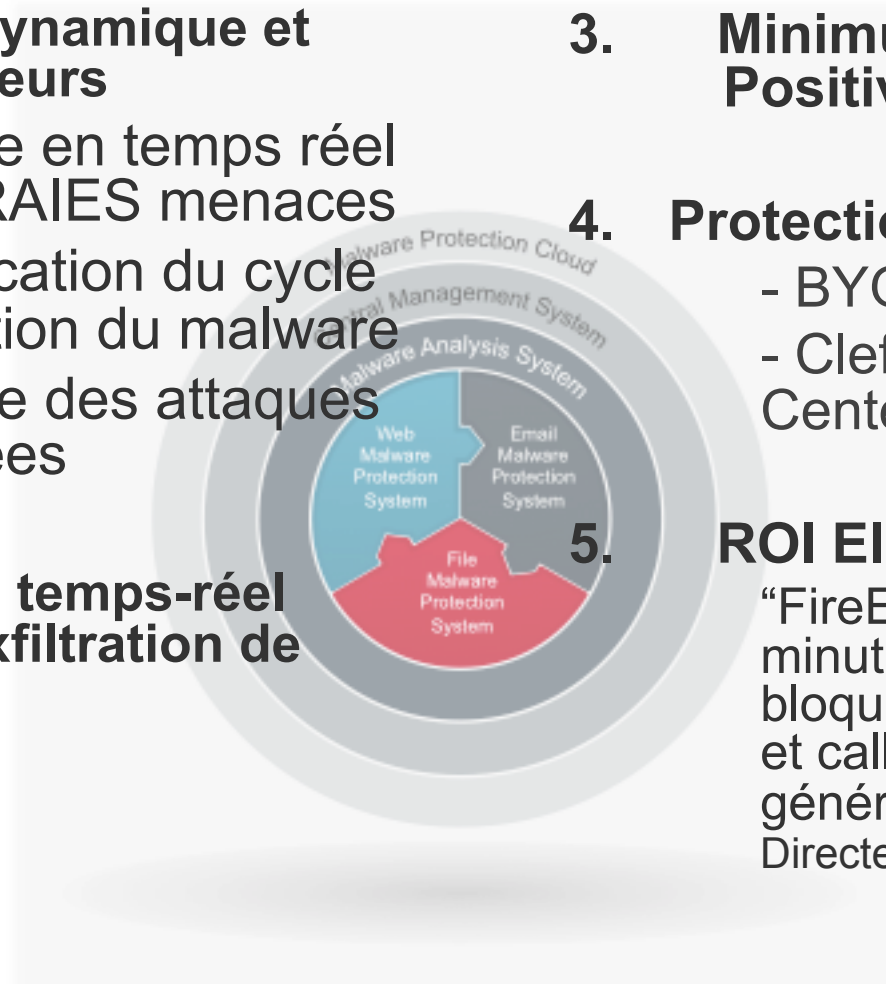
## 3. Minimum de Faux Positives

## 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







Don't trust us, Test us

MERCI

Retrouvez-nous sur le Stand 7

[www.FireEye.com](http://www.FireEye.com)

