APT / Cryptolockers

Pierre Poggi – Country Manager

Pascal Le Digol – Senior Sales Engineer – CISSP

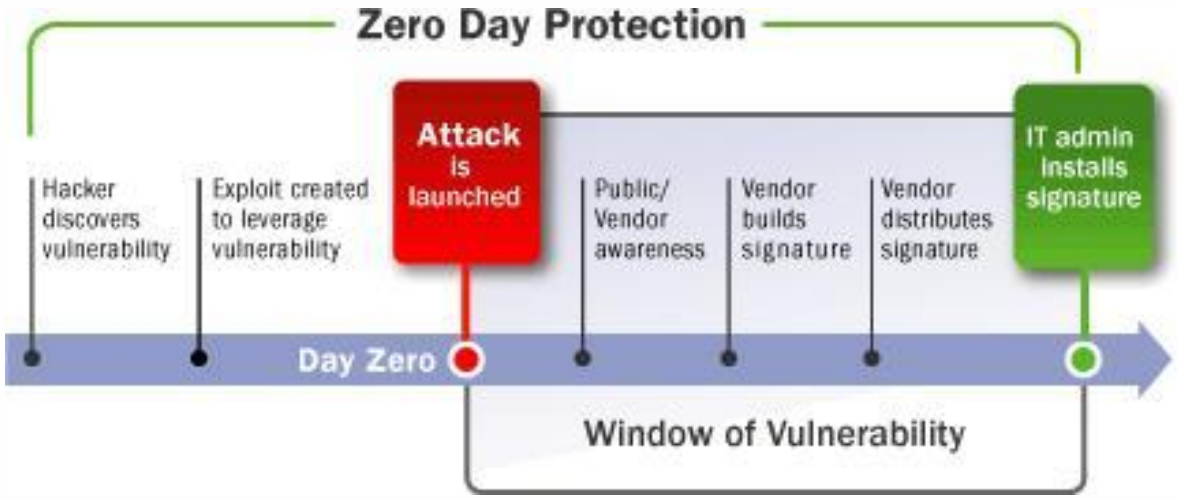
SMART SECURITY

Houston, on a un problème !

- « J'ai un antivirus et un IPS à jour mais je me suis fait infecter malgré tout »

Première raison : Le « Zero Day »

- Pas de correctif sur une faille
- une faille inconnue pour le moment
- Pas de faille…



Deuxième raison : Les technologies évoluent, *y compris celles des hackers…*

- “Antivirus is Dead” Brian Dye Senior VPN of Symantec

Sponsored Links

Norton Coupon Code (2014)
$40 OFF Norton 360. Norton Partner. Norton Antivirus.
Norton.CouponPal.com

Find top Norton Antivirus
Compare prices at BEST-PRICE.com & save up to 75% on Norton Antivirus!
www.Norton-Antivirus.BEST-PRICE.com

Plus de 88% des malwares évoluent pour ne pas être détecté par les anti-virus*

*Malwise - An Effective and Efficient Classification System for Packed and Polymorphic Malware, Deakin University, Victoria, June 2013

Advanced Persistent Threat – **APT**

- Advanced : Utilise les techniques de Malware les plus modernes et les exploits Zero-Day
- Persistent : Il ne s'agit pas d'un hacker/robot opportuniste qui tombe au hasard sur une faille, il y a une vraie volonté de rentrer sur le réseau
- Historiquement ciblant des organismes gouvernementaux et financiers mais se démocratisant aux PME et tout type d'entreprise
- Les antivirus sont <u>insuffisants</u> contre les APT


EVOLUTION OF APT
APT no longer targets huge corporations and nation-states. Now all companies are vulnerable, regardless of size.
January 2010
Operation Aurora
Target: Google
Result: Steal source code
June 2010
Stuxnet
Target: Iran
Result: Affected nuclear-plant operations
March 2011
RSA/Lockheed
Target: RSA and Lockheed Martin
Result: Stole SecureIDs
September 2011
Duqu
Target: Iran, Sudan, Syria, and Cuba
Result: Stole digital certifications
May 2012
Flame
Target: Countries in Middle East
Result: Data gathering and exfiltration
January 2013
New York Times
Target: NY Times
Result: Stole data, corporate passwords
October 2013
Adobe Breach
Target: Adobe
Result: Stole customer information and data
December 2013
Target Breach
Target: Target
Result: Stole customer credit card data

« Cryptolockers »

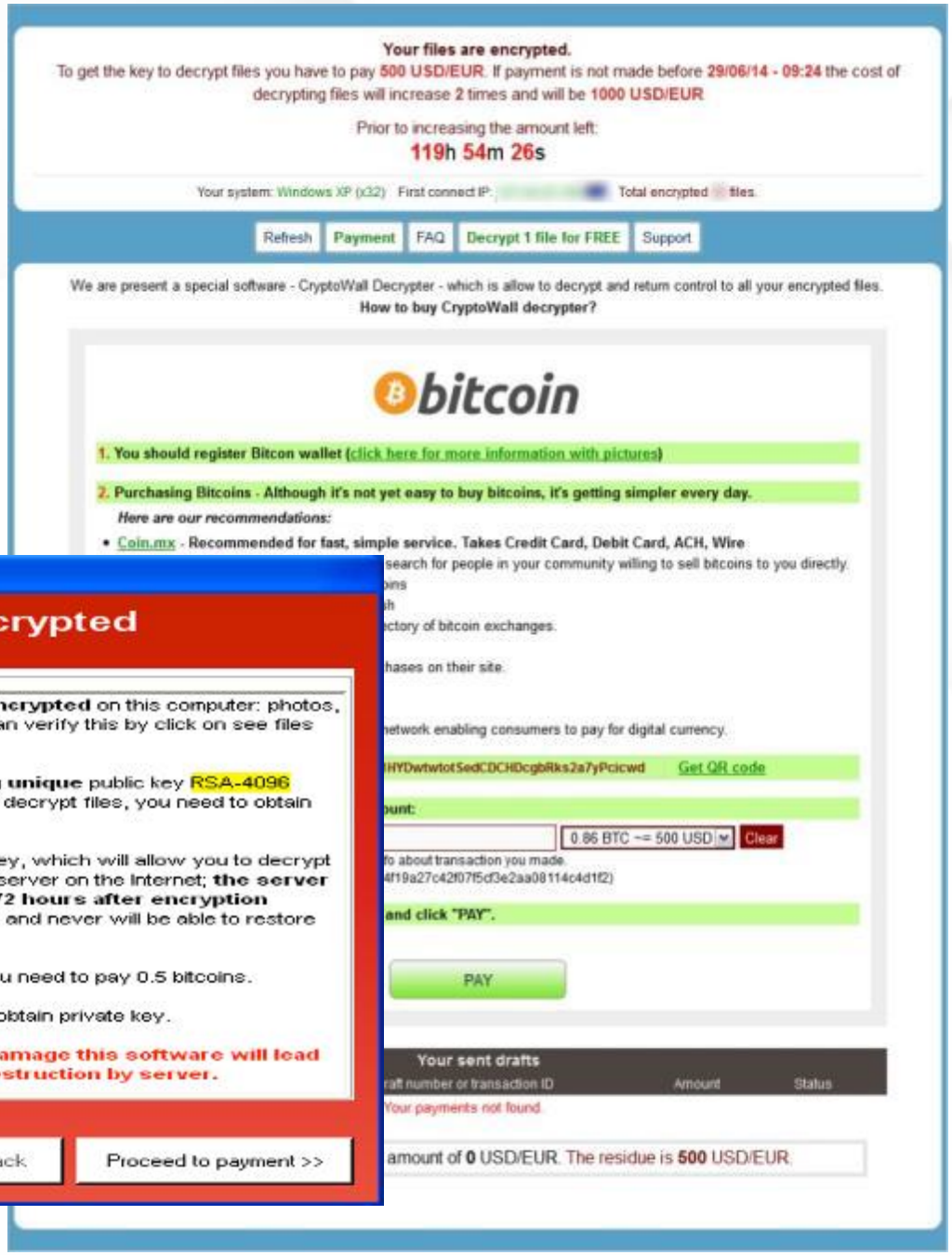
WatchGuard

SMART SECURITY

S.D.I.

TELECOMS - INFORMATIQUE - CLOUD

APT or not APT…



WatchGuard

TECHWORLD News Reviews Features Bl

Hot Topics » Security Cloud Apps Operating Systems Networking

Home > News

Disaster as CryptoWall encrypts US firm's entire server installation

Paying ransom was quicker than backups

By John E. Dunn | Techworld | Published: 15:46, 23 Octol 2014

10 34

Security

In Security:
News
Reviews
Features
How-tos
Slideshows

"Here is a tal cold," announ KnowBe4 in exaggerating

One of his fir advice on ho containing 75 of the hated CryptoWall ransom Trojan

An admin had clicked on a phishing link workstation had mapped drives and pe had quickly jumped on to them to hand

LEMONDE INFORMATIQUE

Rechercher

THÈMES DOSSIERS RÉGIONS EMPLOI AGENDA ÉVÉNEMENTS LIVRES BLANCS PARTNE

EN CE MOMENT : IT TOUR 2014 OPENSTACK SUMMIT PARIS

Test Google Nexus 6 : Le meilleur Nexus à la taille gargantuesque (1e partie...

Windows 10 : Microsoft lâche sa dernière Build truffée de fonctions inédites

Les 10 a secrètes employe

TOUTE L'ACTUALITÉ → SÉCURITÉ → 5,25 MILLIARDS DE FICHIERS PRIS EN ...

Le 01 Septembre 2014

5,25 milliards de fichiers pris en otage par CryptoWall

Le cheval de Troie CryptoWall, un malware de cryptographie utilisé par les pirates pour chiffrer les fichiers des ordinateurs infectés et pour demander des rançons aux propriétaires de fichiers contre la clef de déverrouillage, tiendrait en otage la quantité astronomique de 5,25 milliards de fichiers,

Malicious CryptoWall Ransomware Threat Updated to Version 2.0 with New Obfuscator

Comments (4)

By GoldSparrow in Computer Security

User Rating: (1 votes, average: 5.00 out of 5)

Share: 0 4 0

In the science of updating malware threats, hackers are mostly proactive in their abilities to update threats that have a serious effect on the systems that they infect. One threat that has caused massive issues for computer users is CryptoWall Ransomware due to its ability to encrypt files on an infected system.

CryptoWall ransomware has been a threat that was introduced to computer security experts many months ago where it was noticed to act much like other well-known encryption threats. CryptoWall ransomware's ability to encrypt files and then ask that a fee be paid for a decryption key is a well-thought-out attack on computer users. The crypto-malware that CryptoWall ransomware is has been mostly distributed through fake emails claiming to be a legitimate entity, such as in the cases of fake IRS emails.

Figure 1. - CryptoWall Ransomware Threat message in an updated version

S.D.I.
TELECOMS - INFORMATIQUE - CLOUD

Les Antivirus détectent les cryptolockers…. mais… trop tard!

virustotal

SHA256: b9309e4de239112078113f30a3fd2599cab47e8bd7aa2c91cebc039ed9f30f93

File name: Parcel_Information.exe

Detection ratio: 1 / 54

Analysis date: 2014-08-05 00:41:44 UTC (0 minutes ago)

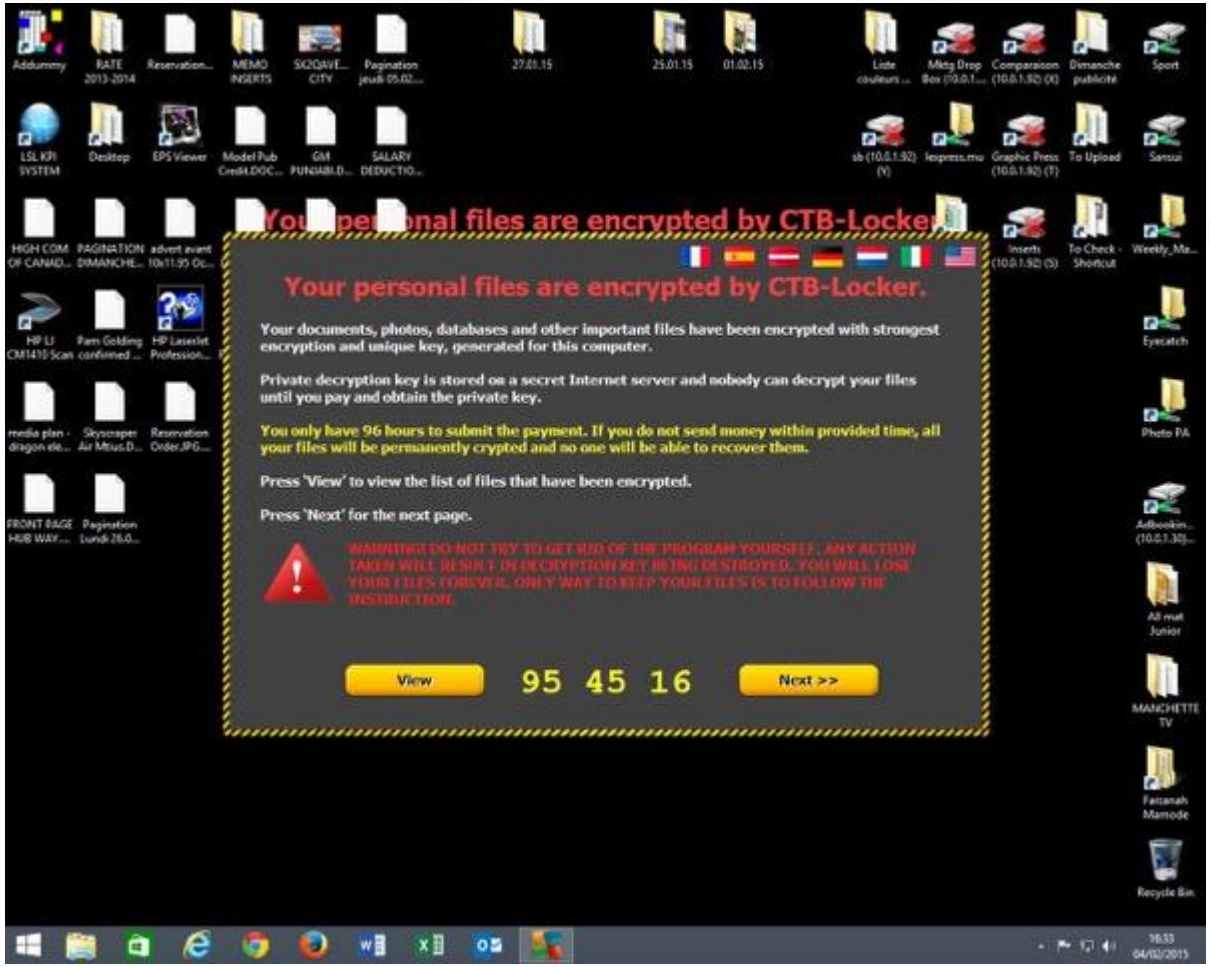
0 0

Analysis | File detail | Additional information | Comments | Votes | Behavioural information

Antivirus	Result	Update
Jiangmin	Pack.Mal.AntiVM	20140804
AVG	✓	20140804
AVware	✓	20140805
Ad-Aware	✓	20140805
AegisLab	✓	20140805
Agnitum	✓	20140804
AhnLab-V3	✓	20140804
AntiVir	✓	20140805
Antiy-AVL	✓	20140804
Avast	✓	20140805
Baidu-International	✓	20140804
BitDefender	✓	20140805

http://www.wtausnz.com.au/cryptolocker-returns-in-a-well-crafted-email-link/

Le « Crypto » du moment…



APTBlocker

Best of Breed Partner - Lastline

- Fondé en 2011
- Redwood City, CA
- Fondé par des professeurs en de plusieurs universités américaines
- Société Privée
- Cloud de Sandboxing et d'émulation de système

- Les créateurs d'**Anubis** System
  - 8 ans de recherches et développement

http://youtu.be/YpEpjoX1Jbk , http://youtu.be/eM7xZyQ0EQQ

Qu'est ce qu'une Sandbox?

Guest OS:

Microsoft Windows

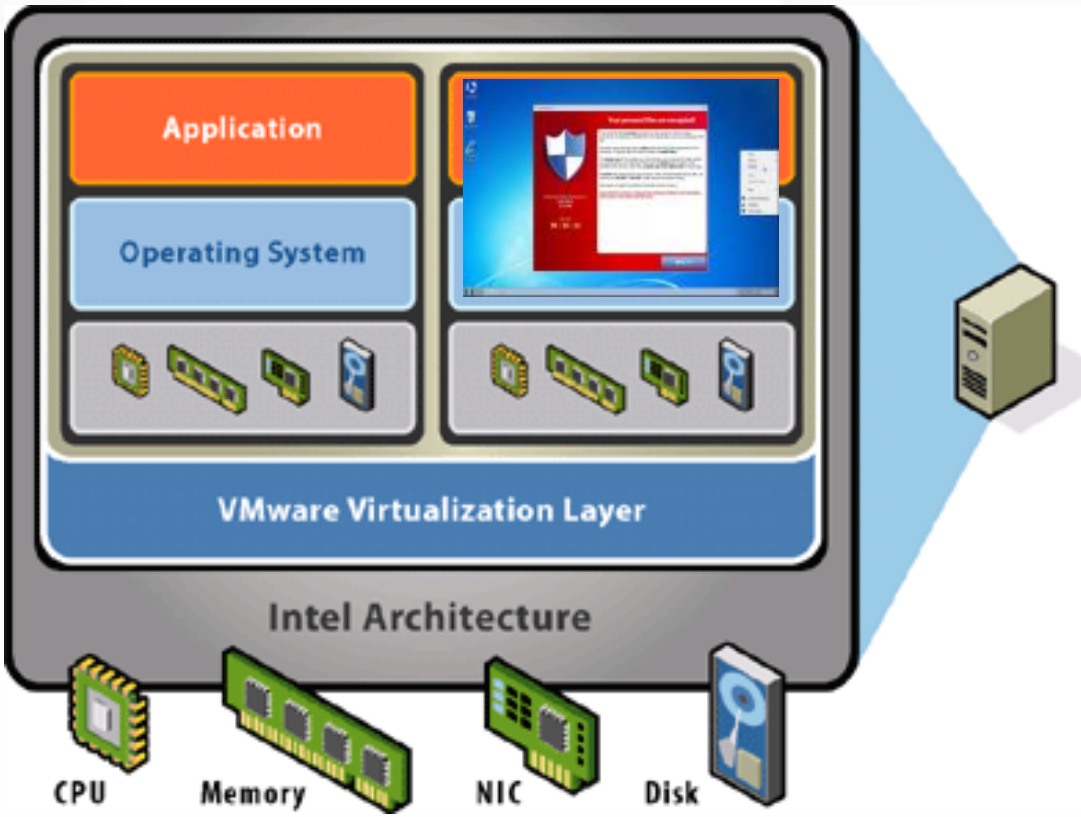
Hyper Visor:

Windows Server Hyper-V

vmware

Hardware:

intel



High-Resolution Malware Analysis

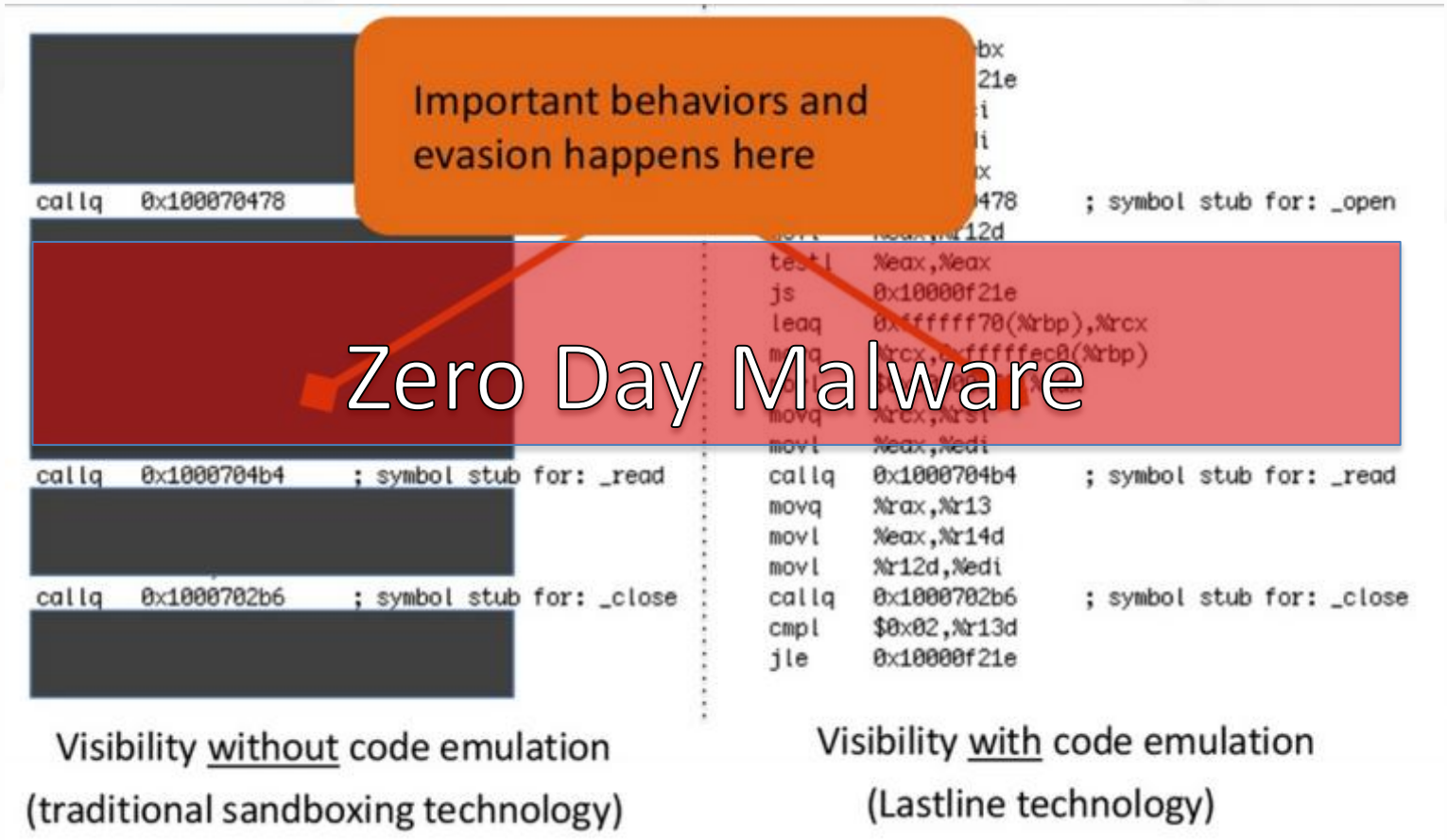
Identifies Evasion Techniques

- Dynamic Evasion
  - Checks for Environment
  - Tool Kits Available for Download

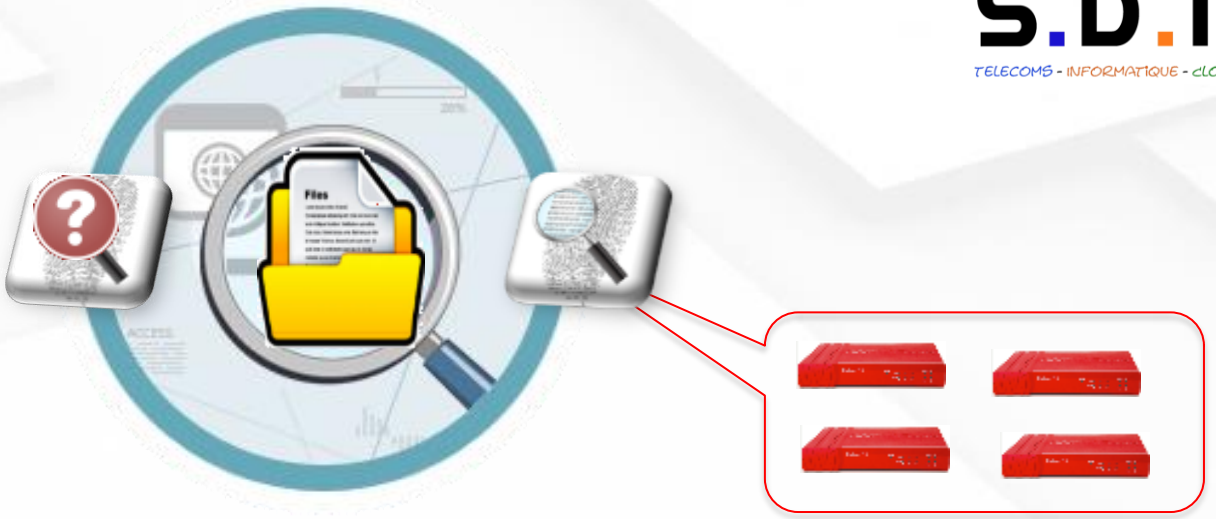
Defeats sandbox and virtual machines

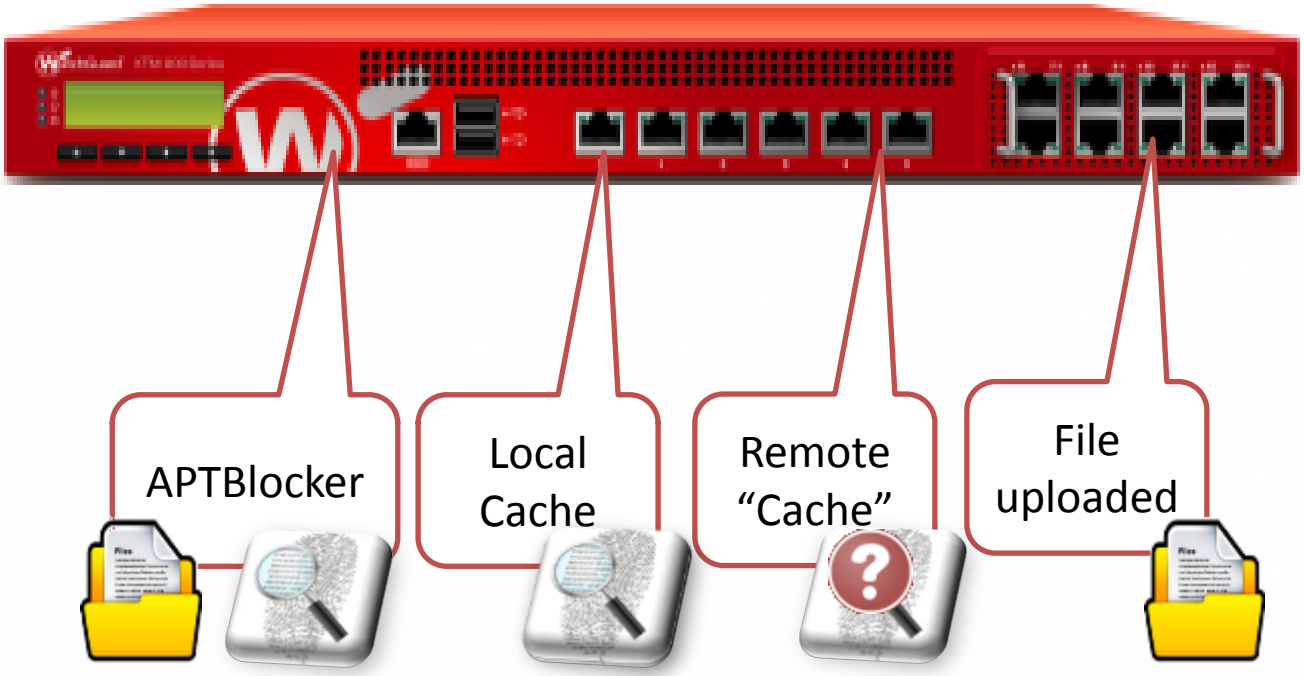
Emulation de Code

- Prévention des évasions



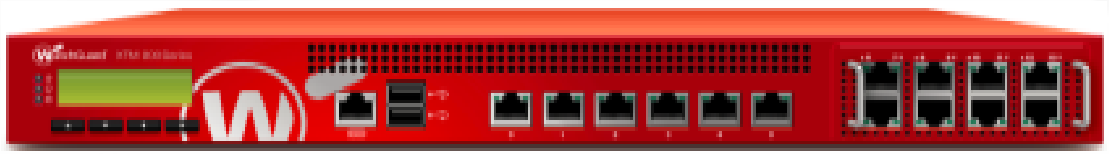
APTBlocker





Unified Threat Management Platform

Security Eco System



Default Threat Protection

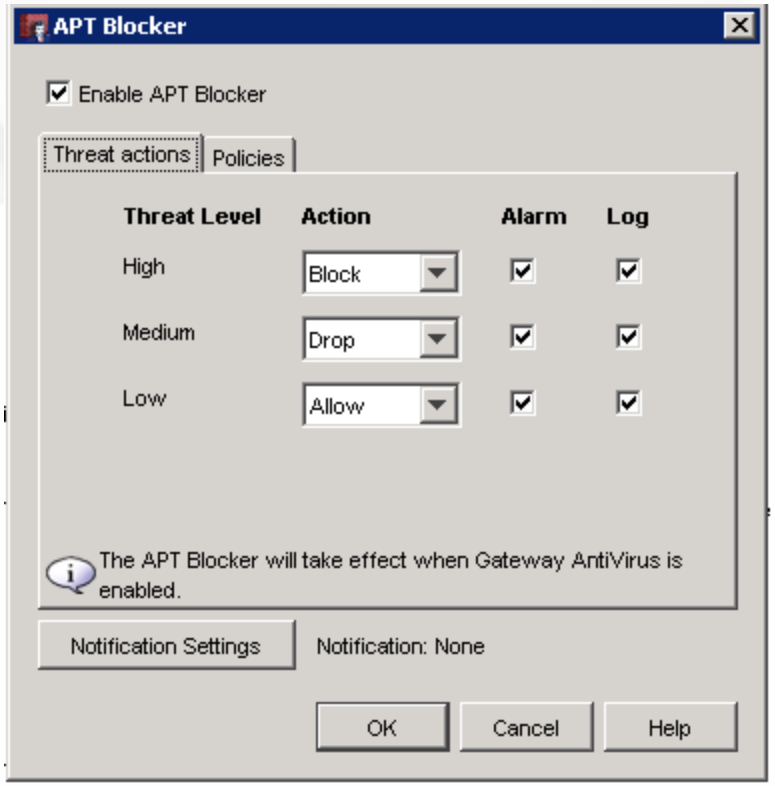
Proxy – Web, Email, FTP

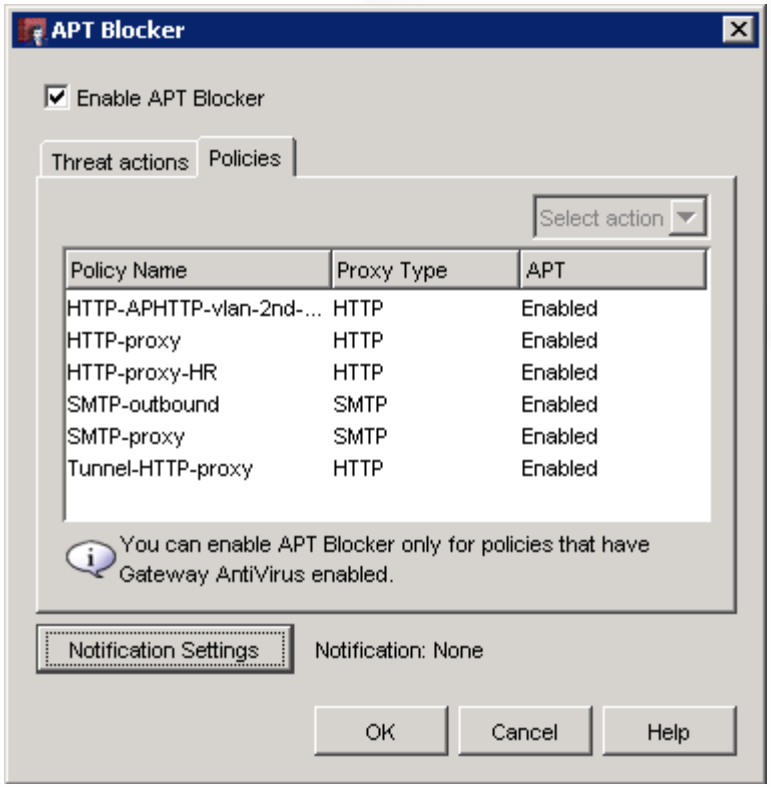
Application Control / IPS

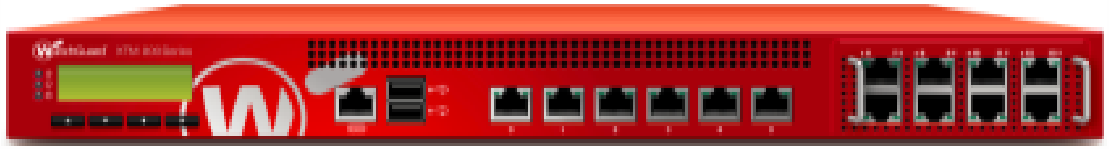
Webblocker / RED / SpamBlocker

AV - Malware APTBlocker

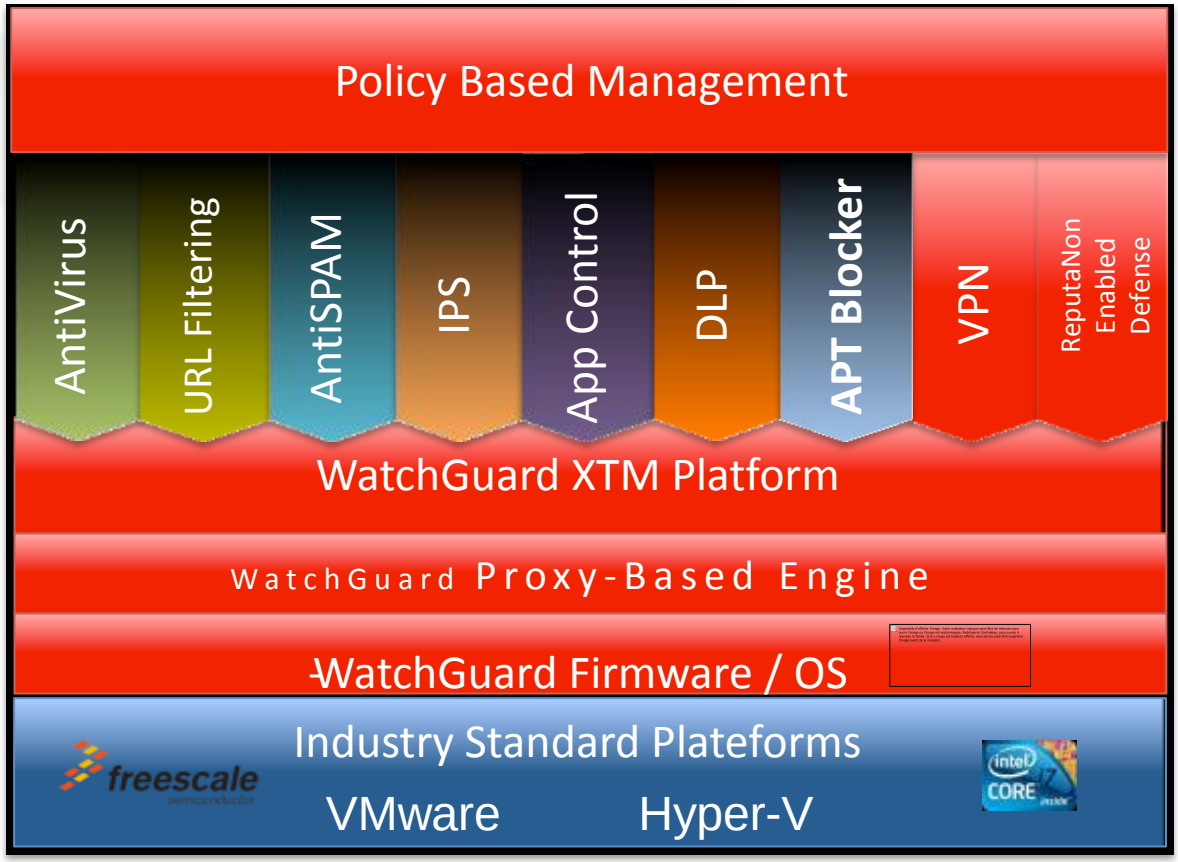
Configuration simple et intuitive







La valeur de WatchGuard : son architecture



Gestion basée sur des règles

Partenariats OEM forts

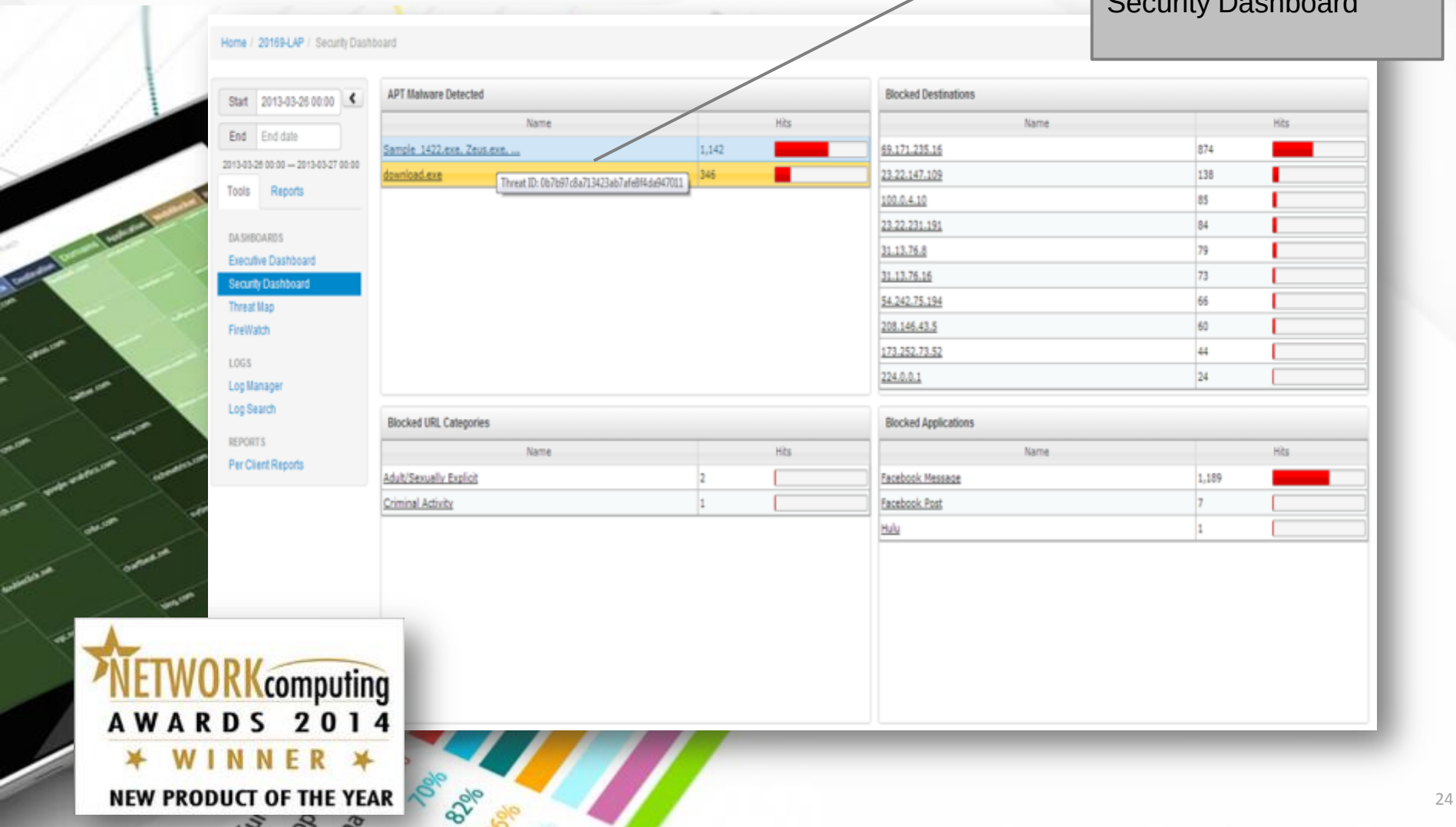
Architecture modulaire

Firmware unique

Plateformes performantes

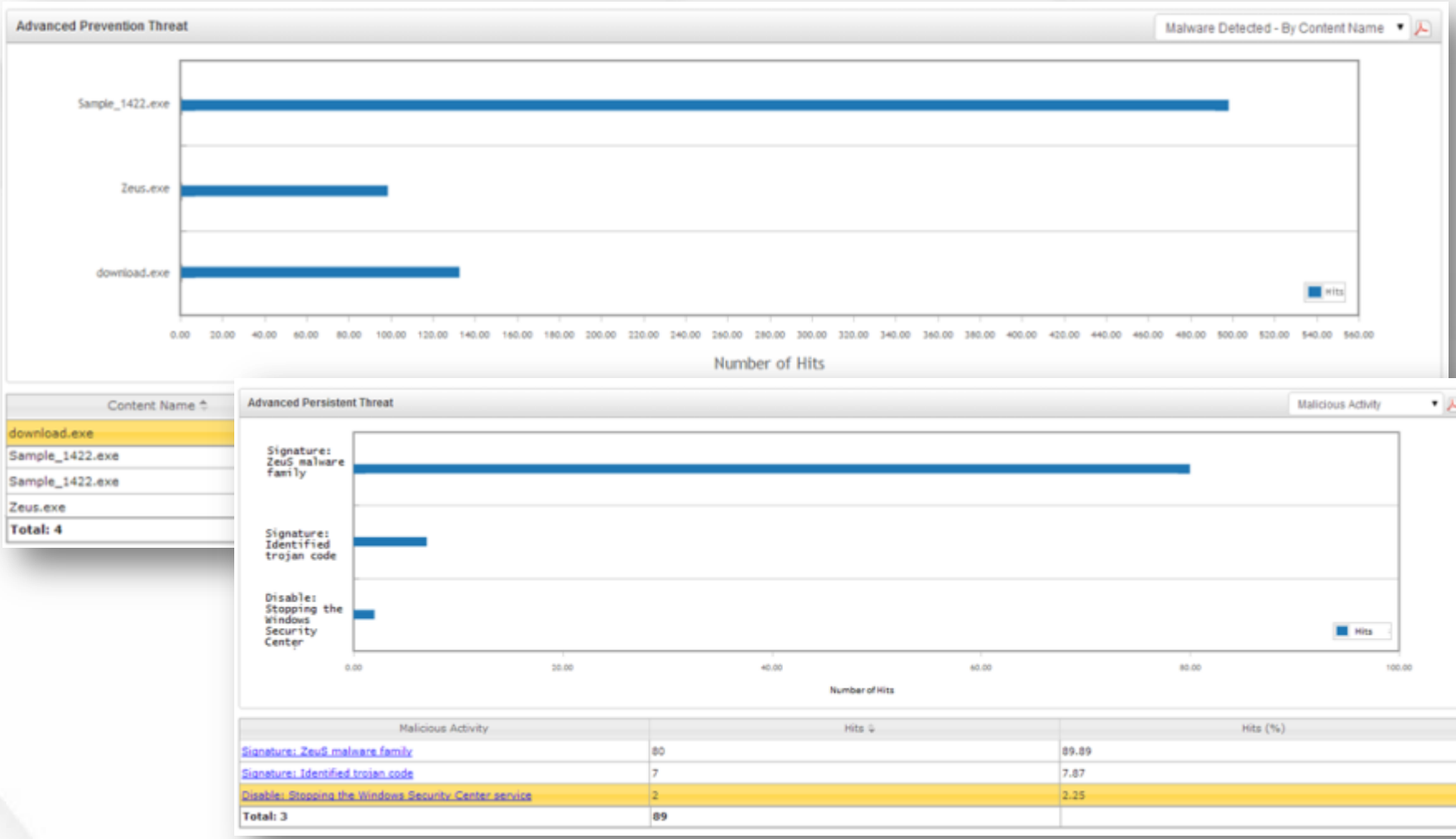
Visibilité dans WatchGuard Dimension

Advanced Malware in Security Dashboard



NETWORK computing AWARDS 2014 WINNER NEW PRODUCT OF THE YEAR

Rapports dans WatchGuard Dimension

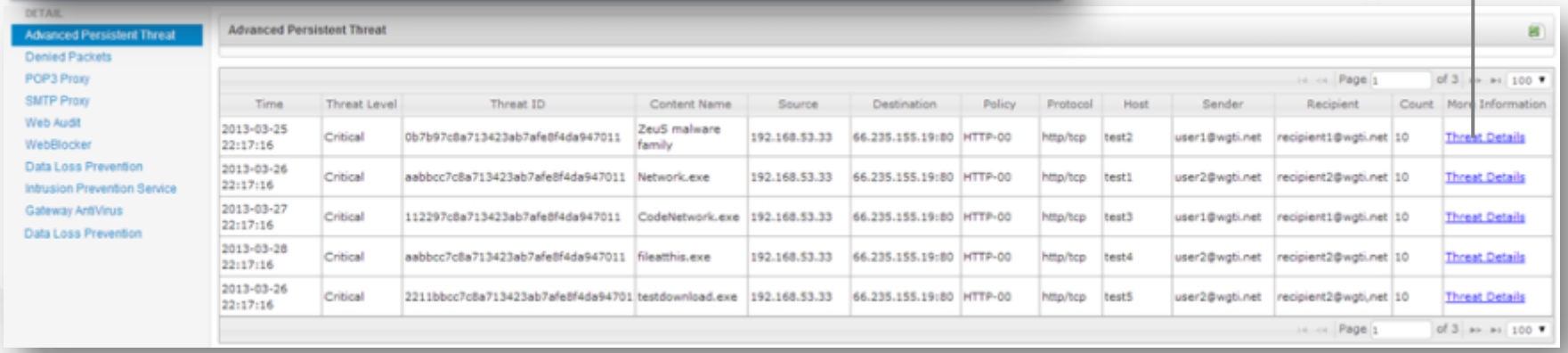


Tout sur l'APT

APT Malicious Activity	
MD5	beaeaf220881d185b7fd1873bf87ed49
Threat Level	HIGH
MIME Type	application/x-pe-app-32bit

Network	Command&Control traffic observed
Autostart	Registering for autostart during Windows boot
Evasion	Trying to detect analysis virtual environment (HDD detection)
Network	Using injected code to hide network activity (dns traffic)
Steal	Reading user's mail server credentials
Disable	Stopping the Windows Security Center service
File	Modifying executable in user-shared data directory
Memory	Writing to the memory of a non-child running process
Settings	Modifying name server (DNS,DHCP) addresses
Evasion	Possibly stalling against analysis environment (sleep)
Evasion	Possibly stalling against analysis environment (loop)

Drill down to find why the activity is determined to be malware



Competitors for Advanced Persistent Threat (APT) Solution of the Year

Check Point	Check Point Threat Emulation
FireEye	Threat Prevention Platform
Fortinet	FortiSandbox
Lancope	StealthWatch System
Lastline	Lastline Previct Advanced Malware Protection
Palo Alto Networks	WildFire
Threat Track Security	Advanced Threat Defense Platform
WatchGuard	WatchGuard APT Blocker

Bonnes pratiques

- Filtrage d'URL, contrôle d'application, Gateway AV
- Mise en place de SandBoxing / Emulation de code (APT Blocker)
- Visibilité : WatchGuard Dimension
- Usage raisonnable et ponctuel d'Internet
- Informer les utilisateurs
- Sauvegarde (rotation, externalisation)

Une gamme de parefeu NGFW & UTM complète

Software Scalability:
Single version of WatchGuard Fireware OS runs on all boxes, including virtual

Increasing throughput to meet business needs

Firebox Extreme E5000*: ETA Planned Q1 2015.
80 – 100Gbps firewall
Consolidated data centers

XTM 2520: Large enterprises and corporate data centers

XTM 15 Series: Large distributed enterprises

Firebox M440: Mid-sized
Port density, PoE

XTM 5 & 800 Series:
Mid-sized businesses and distributed enterprises

XTMv
Four virtual software license versions with full UTM features

XTM 2 & 3 Series:
Small offices, branch offices and wireless hotspots

Firebox T10:
Télétravaille, SoHo, Magasins

Wireless Access Points AP100/200 & AP102
Businesses can harness the power of mobile devices without putting network assets at risk.

*Subject to cancellation or change


WatchGuard
NOTHING GETS PAST RED.
S.D.I.
TELECOMS - INFORMATIQUE - CLOUD
Copyright ©2014
SMART SECURITY