

APT / Cryptolockers

Pierre Poggi – Country Manager

Pascal Le Digol – Senior Sales Engineer – CISSP

Houston, on a un problème !

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

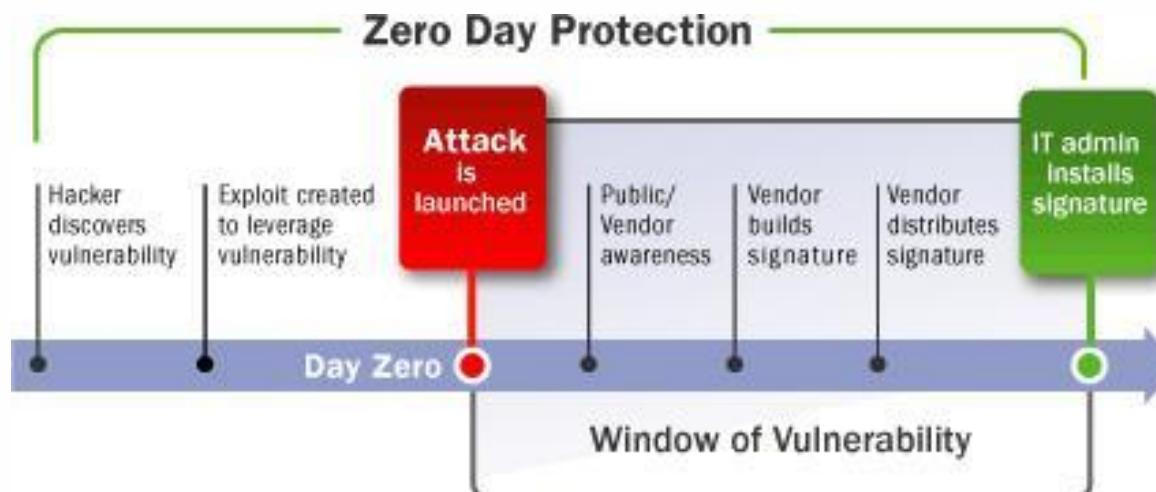


Première raison : Le « Zero Day »

```
10100101010101010101
0101010101010100101
01101001010101010101
10011100101000101001
01100011010101010110
010101010101001001001
0101100101010010100
1010101010101010101010
```

BUG

- 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 insuffisants contre les APT

WHAT IS AN ADVANCED PERSISTENT THREAT?



Targeted

An individual organization, nation-state or even specific technology is the focus. Infiltration is not accidental.



Advanced

An unknown, zero-day attack that has malware payloads and uses kernel rootkits and evasion-detection technologies.



Persistent

It doesn't stop. It keeps phishing, plugging and probing until it finds a way in to serve malware.

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 »





APT or not APT...

Cryptolocker 2.0

Your personal files are encrypted



Your files will be lost without payment on:

11/24/2013 3:16:34 PM

Info

Your **important files were encrypted** on this computer: photos, videos, documents, etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private key**.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.]

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

See files

<< Back

Proceed to payment >>

Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **29/06/14 - 09:24** the cost of decrypting files will increase 2 times and will be **1000 USD/EUR**.

Prior to increasing the amount left:
119h 54m 26s

Your system: Windows XP (x32) First connect IP: Total encrypted files.

Refresh Payment FAQ Decrypt 1 file for FREE Support

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.
[How to buy CryptoWall decrypter?](#)

bitcoin

1. You should register Bitcoin wallet ([click here for more information with pictures](#))
2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.
 Here are our recommendations:
 - [Coin.mx](#) - Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire

search for people in your community willing to sell bitcoins to you directly.
 Options
 Search
 factory of bitcoin exchanges.
 Buy
 purchases on their site.

network enabling consumers to pay for digital currency.

HYDwhtotSeidCDCHDcpbRks2a7yPcICwd Get QR code

Amount: 0.86 BTC = 500 USD

to about transaction you made.
 4f19a27c42f0715d3e2aa08114c4d1f2

and click "PAY".

Your sent drafts
 Draft number or transaction ID Amount Status
 Your payments not found.

amount of 0 USD/EUR. The residue is 500 USD/EUR.



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 October 2014



Security

In Security:
News
Reviews
Features
How-tos
Slideshows

"Here is a tall cold," announced KnowBe4 in exaggerating

One of his final pieces of advice on how to contain 75% of the hated [CryptoWall ransom Trojan](#)

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



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



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



Les 10 astuces secrètes employé

TOUJOU 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 clé 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

By Goldsparrow in Computer Security

Comments (4)

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

Share:

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

What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 2.0.
More information about the encryption keys using RSA-2048 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

What does this mean?

This means that the structure and data within your files have been irrevocably changed; you will not be able to work with them; read them or see them; it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?

Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.

Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?

Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.

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



SHA256: b9309e4de239112078113f0a3fd2599cab47e8bd7aa2c91cebc039ed9f0f93
File name: Parcel_Information.exe
Detection ratio: 1 / 54
Analysis date: 2014-08-05 00:41:44 UTC (0 minutes ago)

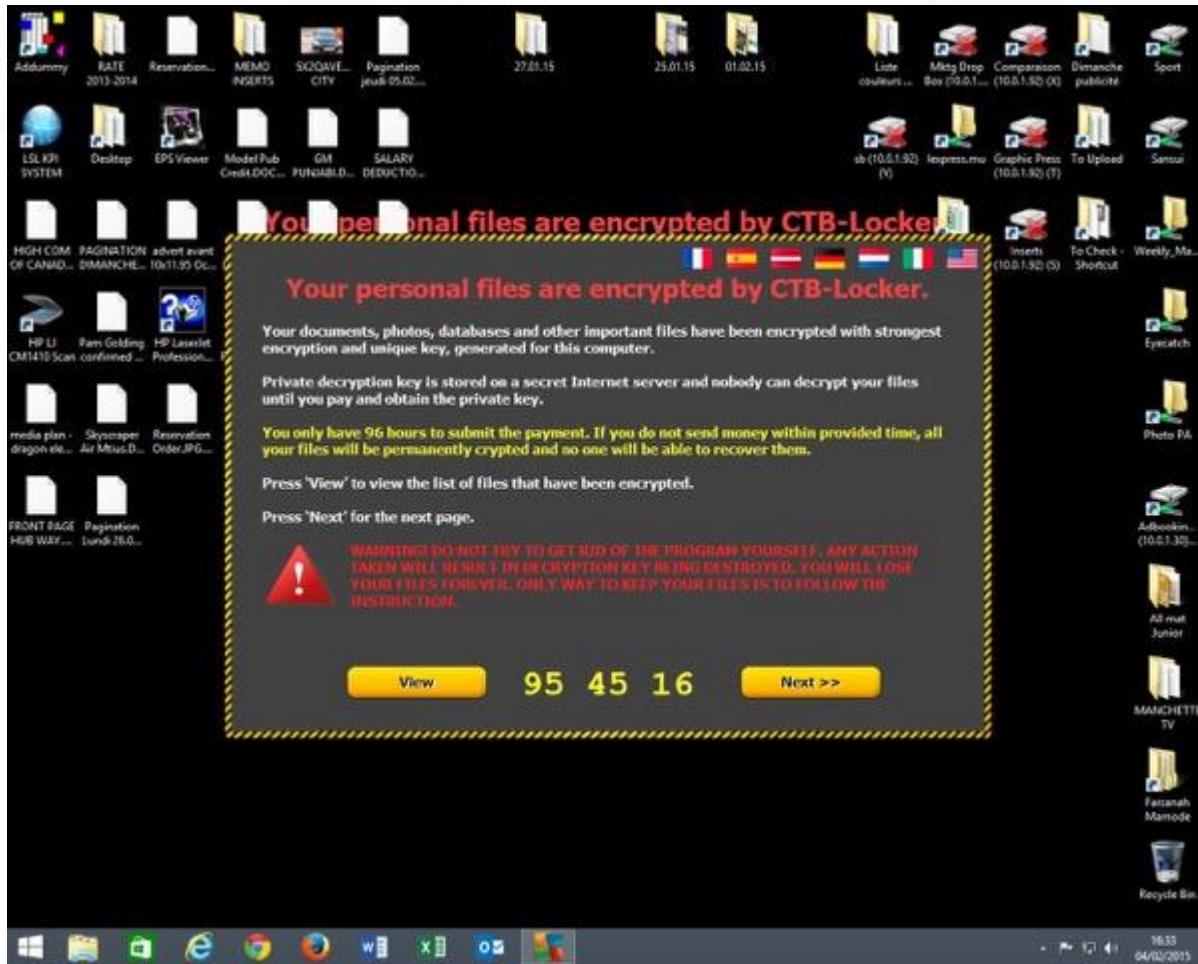


Analysis File detail Additional information Comments Votes Behavioural information

Antivirus	Result	Update
Jiangmin	Pack_Mal_AntiVM	20140804
AVG	✓	20140804
AVware	✓	20140805
Ad-Aware	✓	20140805
AegisLab	✓	20140805
Agnitum	✓	20140804
AhnLab-V3	✓	20140804
AntiVir	✓	20140805
Antiyy-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?

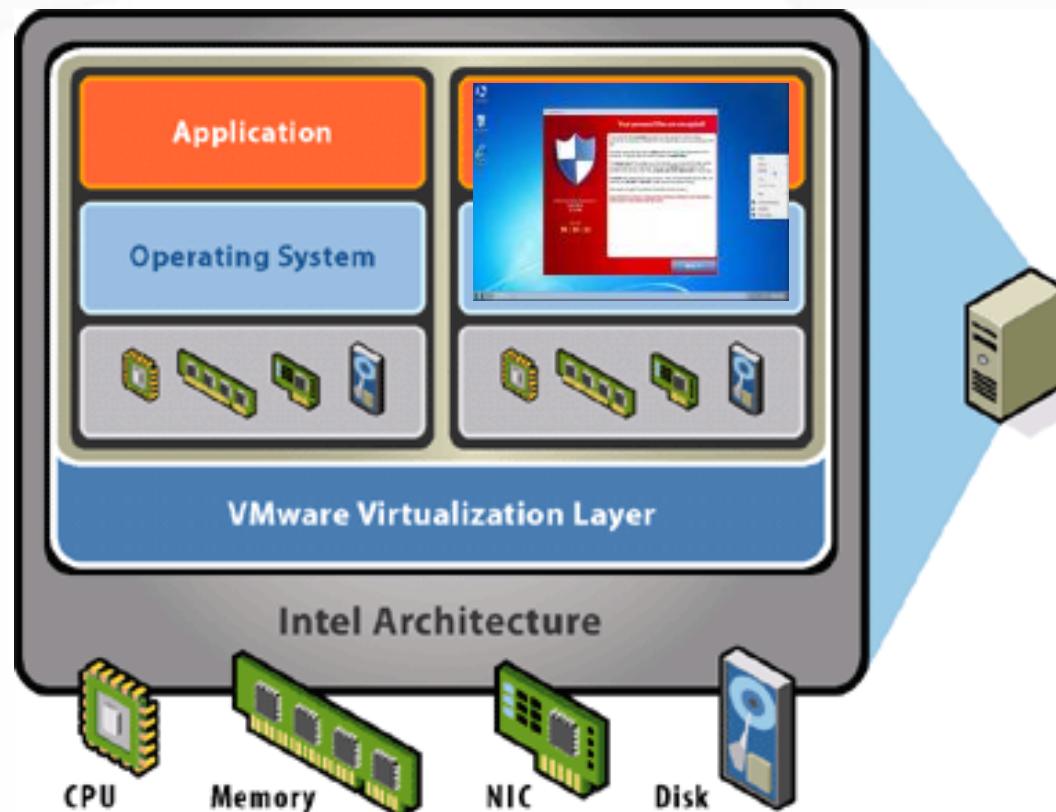
Guest OS:



Hyper Visor:



Hardware:

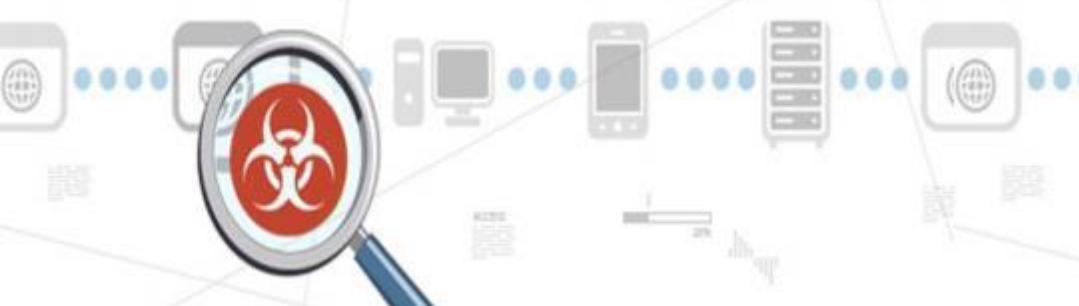


High-Resolution Malware Analysis

Identifies Evasion Techniques

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

Defeats sandbox and
virtual machines



PXCrypter 1.1 Fully undetected

PXCrypter 1.1 build 231

Input Filename:

Change Icon:

Icon Filename:

Adv Settings:

Anti Virtualization (Microsoft VPC,VMware,VirtualBox)
 Anti Debug (Ollydbg,Soft-ICE,IDA,Generic Debuggers)
 Anti SandBoxie/ThreatExpert
 Anti SandBoxes (Norman,Anubis,CW,Generic Sandboxes)

Melt on exit
 Start Hidden (Without GUI)
 Try to Unpack the Executable before Crypting

UPX Packing Mode: Automatic (Recommended)

Overlay Detection/Processing: Automatic (Recommended)

Injection Target: Default Self (Recommended)

Delay: 0 Seconds

Build

Private Version for Current Customers

Emulation de Code

- Prévention des évasions

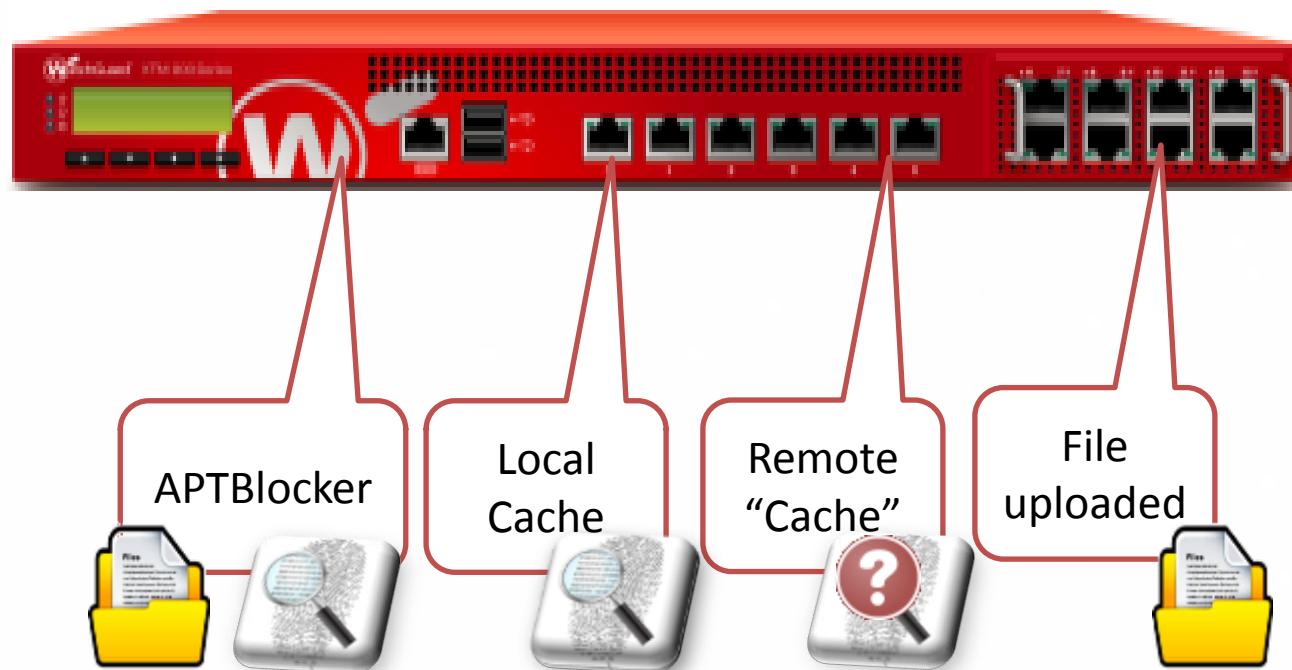
The diagram illustrates the difference in visibility of malware code between two approaches. On the left, under 'Visibility without code emulation' (traditional sandboxing), only the first few assembly instructions of a function are visible: a call to 0x100070478, followed by several redacted blocks of code. An orange callout bubble points to the start of the function with the text 'Important behaviors and evasion happens here'. On the right, under 'Visibility with code emulation' (Lastline technology), the entire assembly code for the function is visible, showing a full sequence of instructions including calls to _open, _read, and _close, along with various memory operations and jumps.

```
callq 0x100070478 ; symbol stub for: _open
testl %eax,%eax
js 0x10000f21e
leaq 0xffffffff70(%rbp),%rcx
movq %rcx,0xfffffec0(%rbp)
movl %eax,%r12d
bxr %r12d,%r13
movl %eax,%r14d
movl %r12d,%edi
callq 0x1000704b4 ; symbol stub for: _read
movq %rax,%r13
movl %eax,%r14d
movl %r12d,%edi
callq 0x1000702b6 ; symbol stub for: _close
cmpl $0x02,%r13d
jle 0x10000f21e
```

Visibility without code emulation
(traditional sandboxing technology)

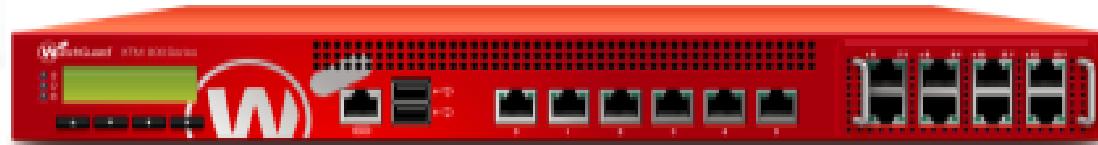
Visibility with code emulation
(Lastline technology)

APTBlocker



Unified Threat Management Platform

Security Eco System



Default Threat Protection

Proxy – Web, Email, FTP

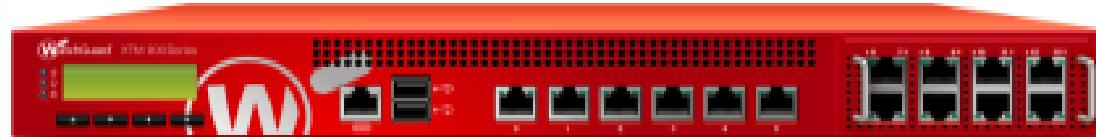
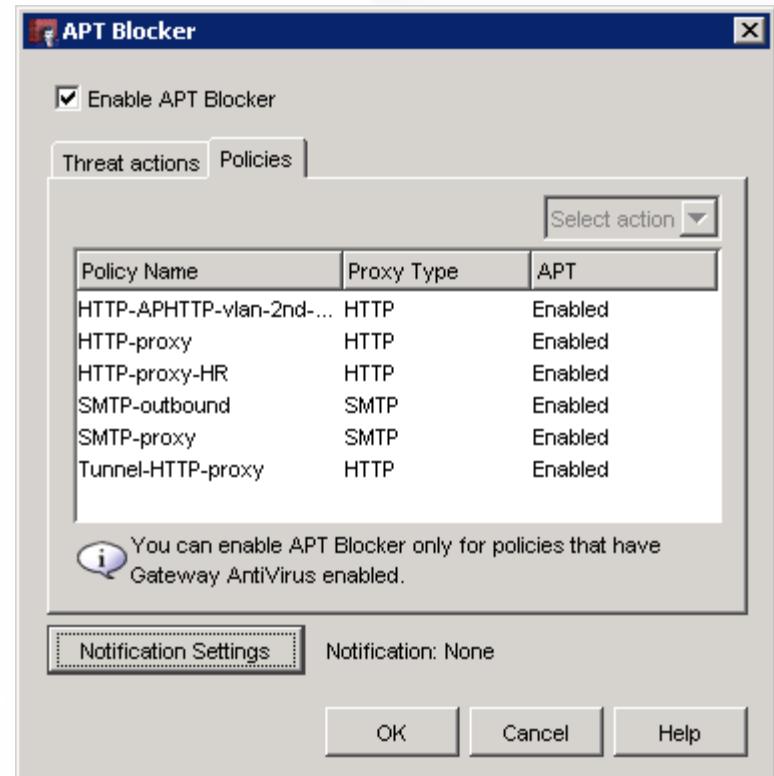
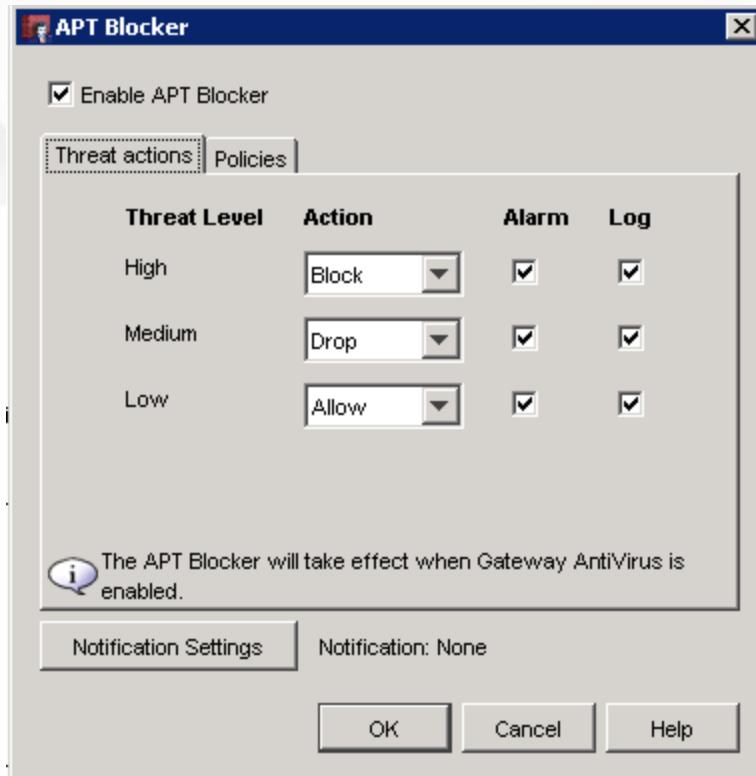
Application Control / IPS

Webblocker / RED / SpamBlocker

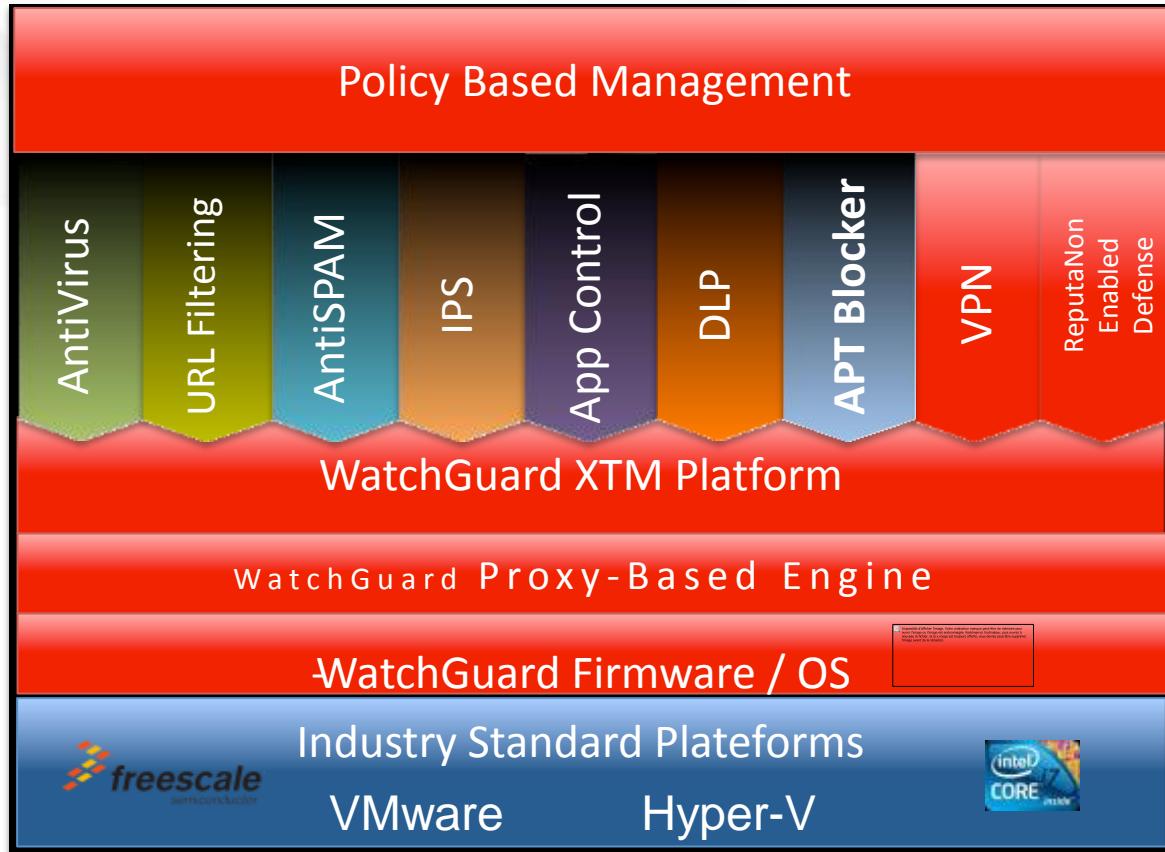
AV - Malware

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

The screenshot shows the WatchGuard Dimension Security Dashboard. On the left, there's a navigation sidebar with links to Home, Dashboards (Executive Dashboard, Security Dashboard, Threat Map, FireWatch), Logs (Log Manager, Log Search), and Reports (Per Client Reports). The main area has four tables:

- APT Malware Detected:**

Name	Hits
Sample_1422.exe, Zeus.exe, ...	1,142
download.exe	346
- Blocked Destinations:**

Name	Hits
69.171.235.16	874
23.22.147.109	138
100.0.4.10	85
23.22.231.191	84
31.13.76.8	79
31.13.76.16	73
54.242.75.194	66
208.146.43.5	60
173.252.73.52	44
224.0.0.1	24
- Blocked URL Categories:**

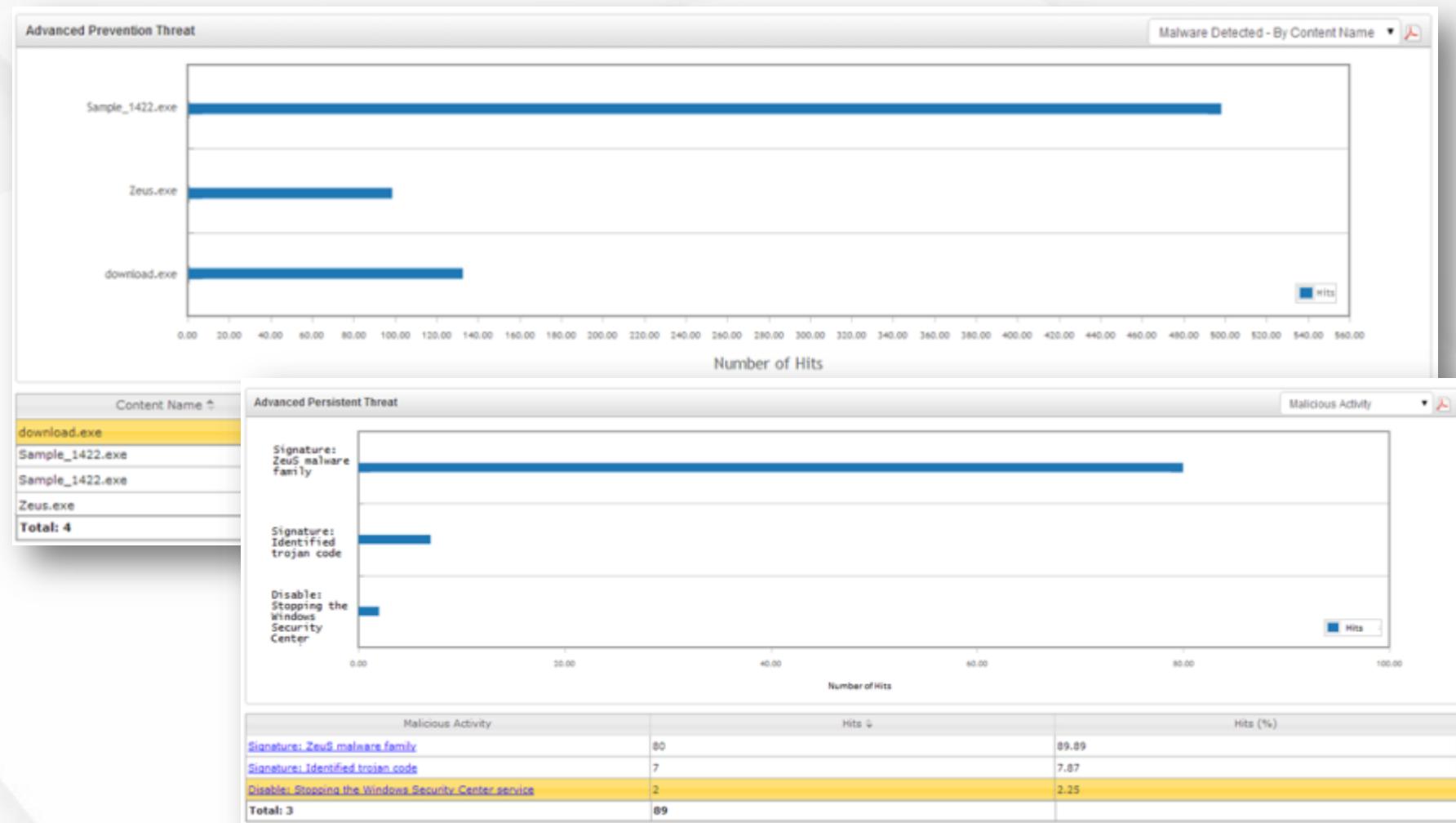
Name	Hits
Adult/Sexually Explicit	2
Criminal Activity	1
- Blocked Applications:**

Name	Hits
Facebook Message	1,189
Facebook Post	7
Hulu	1

Advanced Malware in
Security Dashboard



Rapports dans WatchGuard Dimension



Tout sur l'APT

APT Malicious Activity	
MD5	beaea1220881d185b7fd1873bf87ed49
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)

DETAIL

Advanced Persistent Threat													
Advanced Persistent Threat Denied Packets POP3 Proxy SMTP Proxy Web Audit WebBlocker Data Loss Prevention Intrusion Prevention Service Gateway AntiVirus Data Loss Prevention	Time	Threat Level	Threat ID	Content Name	Source	Destination	Policy	Protocol	Host	Sender	Recipient	Count	More Information
	2013-03-25 22:17:16	Critical	0b7b97c8a713423ab7afe8f4da947011	Zeus malware family	192.168.53.33	66.235.155.19:80	HTTP-00	http/tcp	test2	user1@wgti.net	recipient1@wgti.net	10	Threat Details
	2013-03-26 22:17:16	Critical	aabbcc7c8a713423ab7afe8f4da947011	Network.exe	192.168.53.33	66.235.155.19:80	HTTP-00	http/tcp	test1	user2@wgti.net	recipient2@wgti.net	10	Threat Details
	2013-03-27 22:17:16	Critical	112297c8a713423ab7afe8f4da947011	CodeNetwork.exe	192.168.53.33	66.235.155.19:80	HTTP-00	http/tcp	test3	user1@wgti.net	recipient1@wgti.net	10	Threat Details
	2013-03-28 22:17:16	Critical	aabbcc7c8a713423ab7afe8f4da947011	fileatthis.exe	192.168.53.33	66.235.155.19:80	HTTP-00	http/tcp	test4	user2@wgti.net	recipient2@wgti.net	10	Threat Details
	2013-03-26 22:17:16	Critical	2211bbcc7c8a713423ab7afe8f4da94701	testdownload.exe	192.168.53.33	66.235.155.19:80	HTTP-00	http/tcp	test5	user2@wgti.net	recipient2@wgti.net	10	Threat Details

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



WINNER

Advanced Persistent Threat (APT) Solution of the Year

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

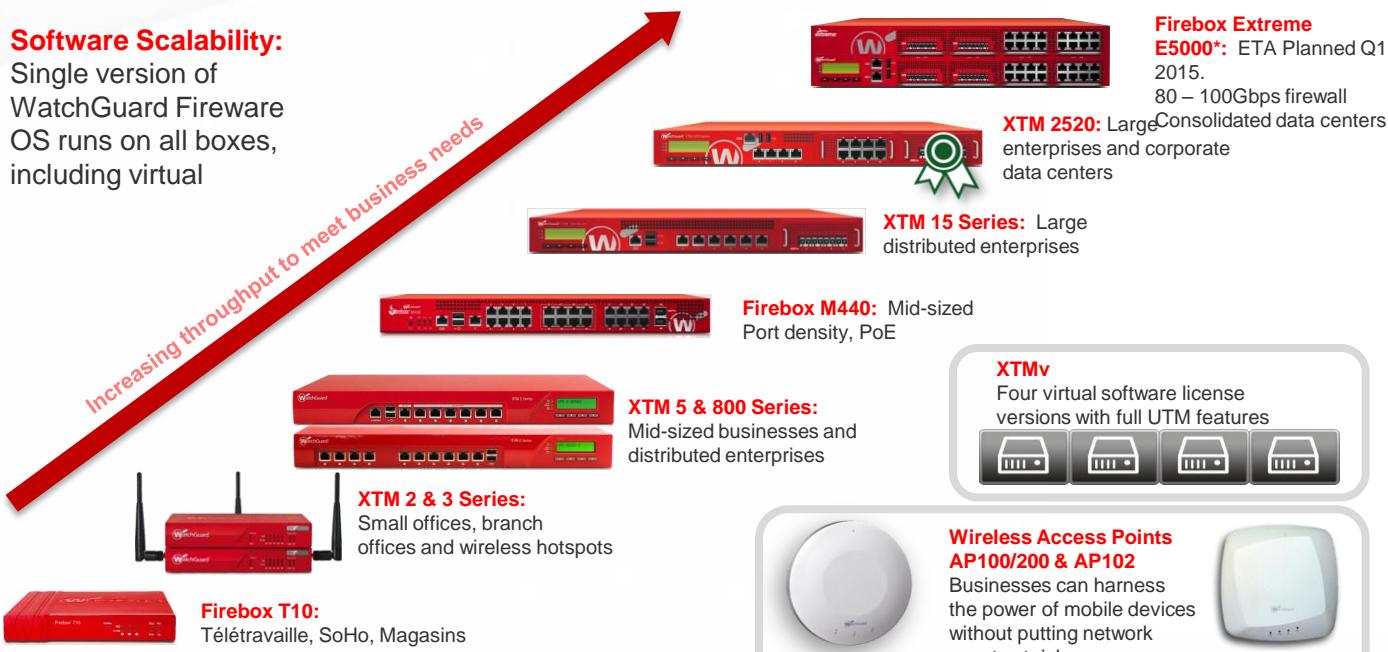
- Filtrage d'URL, contrôle d'application, Gateway AV
- Mise en place de SandBoxing / Emulation de code (APT Blocker)
- Visibilité : WatchGuard Dimension
- Usage raisonnable et ponctuel d'Internet
- Informer les utilisateurs
- Sauvegarde (rotation, externalisation)

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



*Subject to cancellation or change



3
0

**NOTHING GETS
PAST RED.**

S.D.I.

TELECOMS - INFORMATIQUE - CLOUD

