TREND MICRO

Securing Your Journey to the Cloud

Advanced Threat Protection

Deep Discovery

Pierre SIAUT
Business Development Manager

11 Septembre 2012

Hacktivité et cybercriminalité en hausse

Plus fréquent

Plus ciblé

Plus lucratif

Plus sophistiqué

+ 44 % de cyber-attaque

Second Annual Cost of Cyber Crime Study, Ponemon Institute, Aout 2011

PLAYSTATION Network · FBI · DigiNotar Internet Trust Services · MySQL · BFMTV NEWS 24/7 · citigroup · twitter · COMODO Creating Trust Online · RSA SECURITY · NASDAQ · BOEING

- Luckycat, *2012*
- Shadyrat, *2011 (2006)*
- Nightdragon, *2011 (2009)*
- Ghostnet, *2011 (2006)*
- Nitro, *2011*
- Lurid/Enfal, *2011 (2006)*
- Shadownet, *2009 (2008)*

TREND MICRO

De multiples techniques d'intrusion

Adobe alerte sur une faille de sécurité zero day dans Reader et Acrobat

LeMondeInformatique.fr

Edition du 07/12/2011 Réagissez

Adobe travaille sur
vulnérabilité de type
outil de lecture et cr
actuellement exploit
des logiciels malveill

Crédit Photo: D

Acrobat X (1
une corruptio
traitement d
peut conduir
(Centre de r
Exchange on
d'utilisation p

Un premier

L'éditeur con
car la faille a
problème et

Clubic > Actualités informatique > Sécurité informatique

clubic.com

// Le malware Duqu exploite une faille zero-day de Windows

Publiée par Audrey Oeillet le Mercredi 2 Novembre

L'enquête concernant W32.Duqu, le nouveau malware qui inquiète le Web mondial, progresse : des
le ver contaminait les PC infectés. Une faille jusque-là
rte d'entrée.

Using Metasm To Avoid Antivirus Detection (Ghost Writing ASM)

January 25th, 2012 | Author: r3dy

Building Our Malicious Executab

First we will build the malicious executable using msfpay

```
$ ./msfpayload windows/meterpret
LPORT=443 R > raw_binary
```

In the above command you should change '192.168.
victim to connect back to.

The Metasm Ruby Library

Now that we have created a "raw" binary file we have
language or Assembly Code. To do this we will use the
the metasploit framework. In order for the library to fu
and metasm directory into your system's ruby installat

```
cd ~/tools/metasploit/lib/metasm
cp -a metasm.rb metasm /opt/loca
```

TechKranti Information Revolution

FEB 23

Make Trojan Fully Undetectable (FUD) using Xenocode

A few weeks before, we had posted on how you can make your trojan using LostDoor. But the problem with the so formed trojan is it being detected by almost all AV softwares. We know that after learning to make your own trojan, the next thing you must've exhausted your bandwidth searching for is: "How to make a Trojan undetectable?" Well here is the answer.

First of all you'll have to download Xenocode (Never heard of it? We can't help it google it)

Xenocode is a set of application virtualization and portable application creation technologies developed by Code Systems Corporation.
Applications are packed into single executable files that can be executed instantly on any Windows desktop (so called "portable apps"). The technology therefore emulates only the operation system features that are necessary for the application to run. Applications can be deployed using existing infrastructure, software deployment tools, the web or USB keys. The virtualized application runs independently from other software that is installed on the host PC so there are no conflicts between different versions or DLL files.

Well, reading the above introduction must've got you acquainted you with xenocode application. You might be wondering, how this application will help you in making your Trojan undetectable.

Xenocode creates a virtual operating system for processing the files you have virtualized and hence it completely overwrites your code. As you may know, AV softwares use virus signatures to identify viruses. There are ways in which you can make a trojan undetectable by modifying the Hex code, but it is very tedious. Using xenocode alleviates the pain to a negligible level. The only pain you will have is to grab a full version of the application. Keep in mind that trial version xenocode does not create virtual applications. When you will click on the build button, it will prompt you to purchase license. We hope you understand what we mean to say implicitly.

23 FÉVRIER 2012 • ÉCRIT PAR CANAL 311

2012: début de l'ère des guerres cybernétiques

Like Tweeter 0 +1 0 Share

Soyez le premier à commenter!

Nombreaux spécialistes de la sécurité informatique mettent en garde contre les guerres cybernétiques qui risquent de voir le jour pendant l'année 2012.

De nombreuses attaques pourraient être mises sur pied grâce aux avancées technologiques réalisées en matière de vol de données et d'espionnage.

Les États-Unis, le Royaume-Uni, l'Allemagne, l'Inde et la Chine disposent déjà d'unités spéciales de hackers et de centres techniques pour protéger leurs bases de données stratégiques et être en mesure de faire face à d'éventuelles cyberattaques.

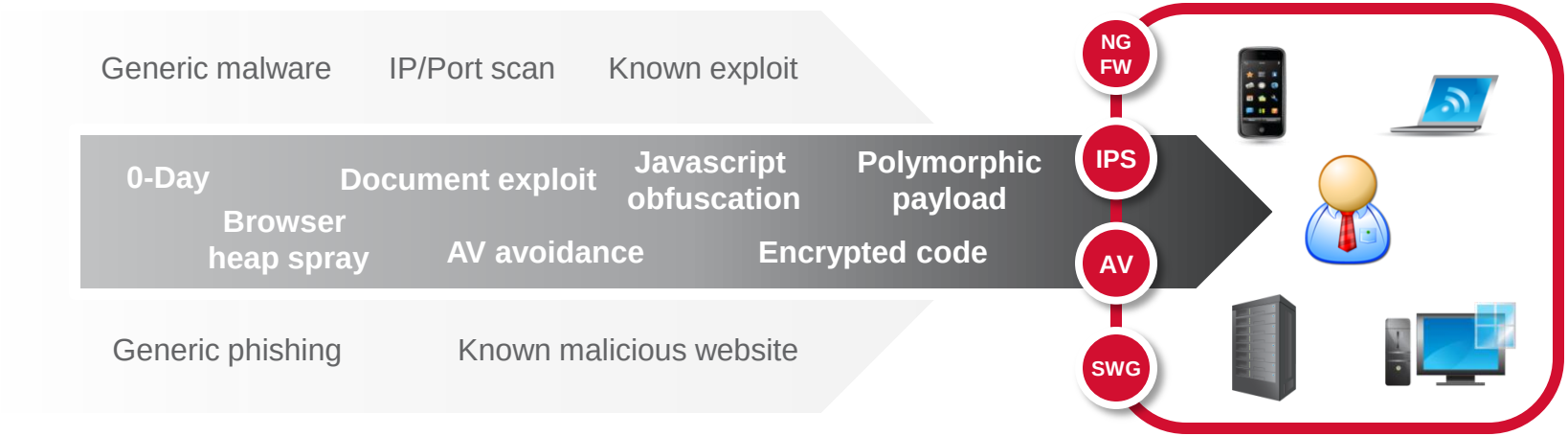
L'expert Loren Thompson a écrit dans la revue Forbes que l'échelle et l'intensité de l'offensive cybernétique chinoise contre les États-Unis étaient devenues bien trop virulentes pour que Washington l'ignore, et tant que Pékin n'affichera pas son intention de la minimiser, les Américains devront prendre des mesures plus percutantes. Au cours de ces deux dernières années, les spécialistes ont relevé une hausse du nombre d'attaques informatiques visant à dérober des données classées secrètes à plusieurs agences gouvernementales,

corporations, entreprises du secteur de la défense et organisations scientifiques, résume le magazine PCWorld. Rick Ferguson, directeur de recherche chez Trend Micro, explique que des programmes de logiciels malveillants tels que les virus Stuxnet et DuQu, conçus pour faire de l'espionnage industriel, sont de bons exemples de ce qui se prépare. Toutefois, il assure que ce type d'attaques exige des compétences professionnelles de haut niveau et un soutien financier conséquent.

De nombreux spécialistes conseillent déjà aux entreprises et aux gouvernements de prendre très au sérieux la menace de cyberattaques réalisées au moyen de logiciels moins sophistiqués, comme pour les opérations Aurora, Shady RAT ou Nitro. Ces « outils d'administration à distance » (RAT, Remote Administration Tool en anglais) ont, ces dernières années, affecté des dizaines d'organisations dans le monde entier.

Publié par Pressenza

Des brèches existantes dans le SSI



98 % des attaques viennent de l'extérieur
- Exploitation de vulnérabilités, 81 %
- Utilisation de malware, 69 %

Verizon Data Breach Investigation Report 2012

Deep Discovery

Visibilité temps-réel de la sécurité du SI

- 80+ protocoles décodés : HTTP, SMTP, CIFS, P2P, IM…
- Détection des documents scriptés, vulnérabilités navigateur...
- Moteur anti-malware avec analyse heuristique
- Analyse des flux réseau : IP, URL, domaine…

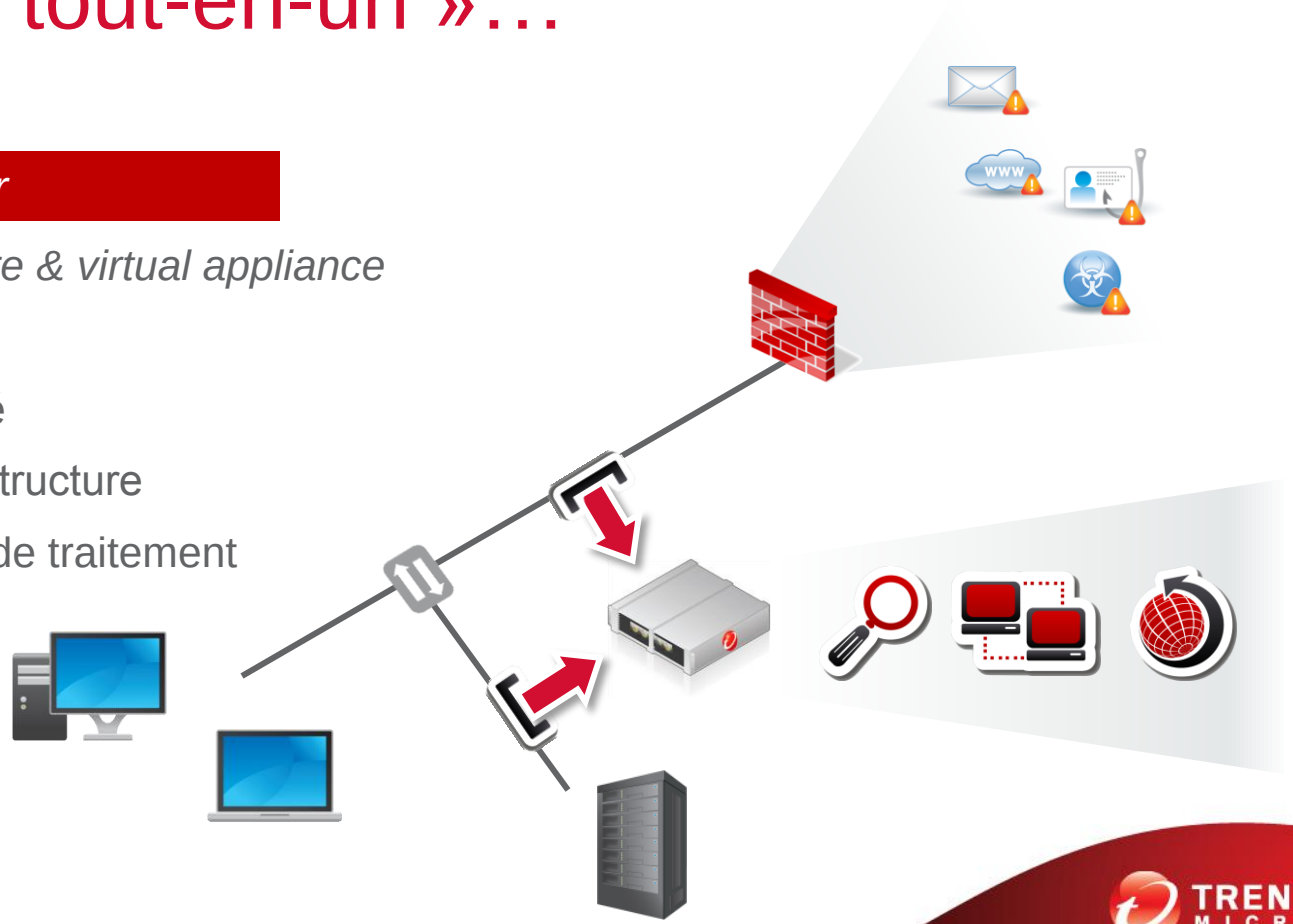
Protection contre les menaces avancées

- Simulation des fichiers à risque en environnement virtualisé
- Corrélation des évènements générés pour éviter les faux positifs

Protection « tout-en-un »…

Deep Discovery *Inspector*

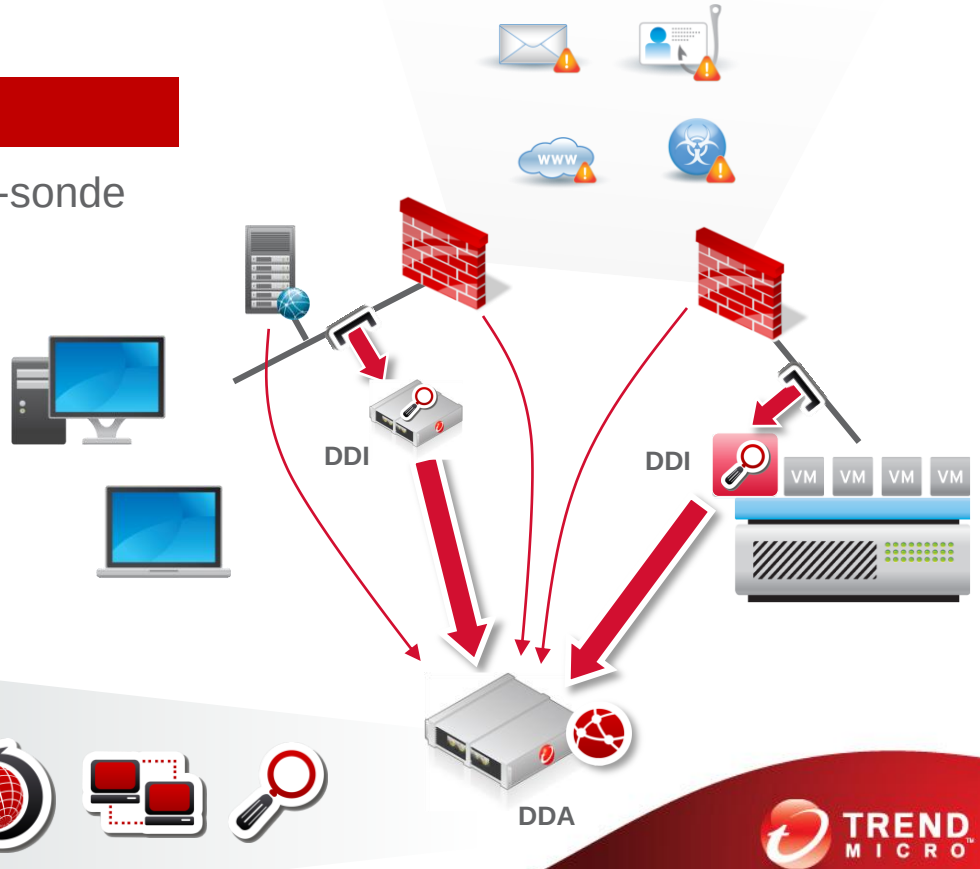
- Modèle *harware, software & virtual appliance*
- Tout embarqué
- Performance et efficacité
- Aucun impact sur l'infrastructure
- Jusqu'à plusieurs Gbps de traitement



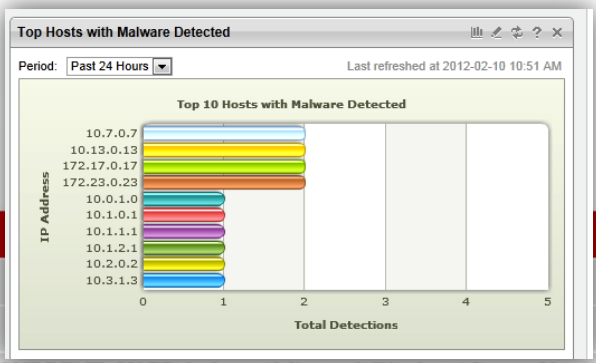
… ou un écosystème global

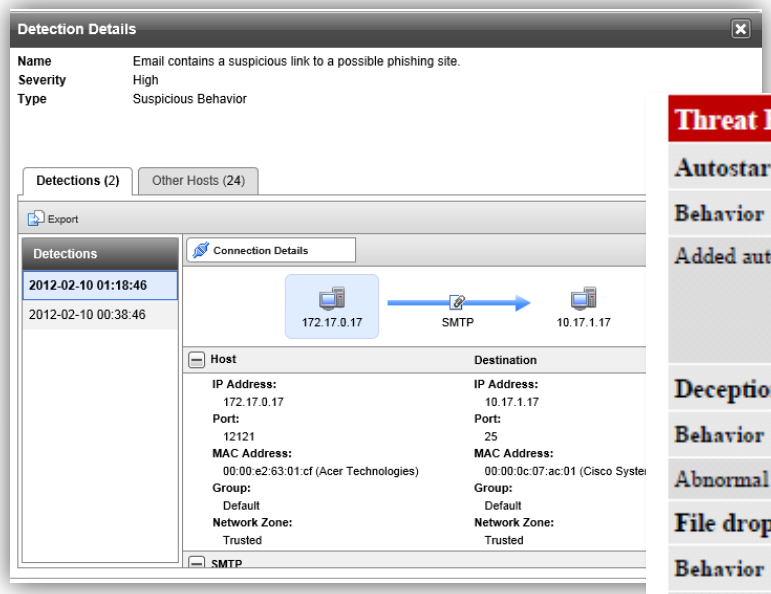
Deep Discovery *Advisor & Inspector*

- Administration & reporting centralisée multi-sonde
- Version hardware ou software
- Détection d'évènement suspicieux
- Multi « sandbox » personnalisées
- Plugin pour les solutions Trend Micro*
- Intégration SIEM existant



Simplicité d'analyse





Threat Behaviors by Category

Autostart or other system reconfiguration

Behavior	Details
Added autorun in registry	KEY: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\{24E47041-7491-AD41-EEE3-FB62C3F3D870}] DATA: ["%APPDATA%\Xuhov\umhu.exe"] TYPE: [REG_SZ]

Deception, social engineering

Behavior	Details
Abnormal version info	The file has no company information.

File drop, download, sharing, or replication

Behavior	Details
Deleted self	The executable "%Virus%\0d23b397aea26dd2579aff9ca0d09582f0c6537f.exe" will remove itself once executing.

Process, service, or memory object change

Behavior	Details

172.17.0.17

IP Address: 172.17.0.17 Hostname: 172.17.0.17
MAC Address: 00:00:e2:63:01:cf Group: Default

Export Total: 5

Severity	Threat	Type	First detected	Last detected	Detections
High	Email contains a suspicious link to a possible phishing site.	Suspicious Behavior	2012-02-10 00:38:46	2012-02-10 01:18:46	2
High	Email message contains a suspicious link to a possible phishing site	Malicious Behavior	2012-02-10 00:38:46	2012-02-10 01:18:46	2
Informational	Web Reputation Services detected a suspicious URL.	Web Reputation	2012-02-10 00:58:50	2012-02-10 00:58:50	1

TREND MICRO

Soyez prêt

Renforcez votre équipe sécurité

- Solution automatisée et dynamique
- Détection des menaces sur de multiples vecteurs
- Accès détaillé aux logs & rapports d'analyses

TrendLabs

Threat Intelligence *inside*

- Accès aux informations détaillées sur vos menaces
- Profitez de l'expertise Trend Micro de façon automatisée

TREND MICRO

TREND MICRO

Securing Your Journey to the Cloud

Demo