

Welcome to Virtual Worlds

*By François Paget
McAfee Avert Labs*

About the Author

François Paget is one of the founding members of McAfee's Avert Labs research group, which started in 1993. For 12 years he was in charge of analyzing new threats, identifying them and making modules available for detecting and eliminating them. His main responsibility has been researching new generic and heuristic detection methods for 32-bit Windows environments. Today, François conducts a variety of forecast studies and performs technological monitoring for his company and for some of their clients. He focuses particularly on the various aspects of online financial fraud.

In 1991, he was the leader of the "Virus Group" within CLUSIF (Club de la Sécurité de l'Information Français [French Information Security Club]). Now, as the Secretary-General of this association, François is currently involved with their "Threats" team.

François is a regular conference speaker at various French and international events in this field. In 2006, he published a reference work through DUNOD, addressing current malware problems. He is also a contributor for several collective works related to information system security.

Contact Details: 30, avenue Lacour, 95210 Saint-Gratien, France, phone +33-1-47625620, e-mail francois_paget(at)avertlabs.com.

Keywords

MMORPG, Metaverse, Virtual World, Malware, Keylogger, Identity Theft, Phishing

Welcome to Virtual Worlds

Abstract

Tens of millions of people on our planet share their existence between two worlds: the real world as we all know it and one of the many virtual universes accessible from the Internet. These universes are highly coveted today. While at first, crime had adapted to the use of the Internet in its most conventional aspects, it now seeks to profit from a parallel economy in full expansion.

The first part of this document will introduce you to these parallel worlds with a summarized overview of the opportunities and their related economic aspects.

Although gaming and socialization are highlighted in these universes, money rules supreme. Cybercriminals understand that. From both the outside or from within, they adapt their methods and invade these places. Here too, the chance of making money arouses great interest.

What was unthinkable a few years ago has become a reality; virtual goods, like gold coins, armor, characters or islands, are now worth a great deal in the "real world". All means to obtain them are valid. The second part of the document deals with conventional malicious programs (viruses and Trojans) related to these environments.

Through some examples, the third part of our document addresses some more tragic and disturbing topics: parallel financial networks, sex and prostitution.

To conclude, in the fourth section, we will discuss some programming techniques and see how some mischief can be carried out by means of scripts or exploits. In this initial version of a document that will evolve over the course of the next few months, we will address only the Linden Script Language of Second Life. Many other trails remain to be studied, and the veil has only been partially lifted on a phenomenon that we must explore in more depth throughout these next few years.

An Introduction to Virtual Worlds

At the crossroads of massive multiplayer online games, social networks and geographic information systems, virtual worlds have experienced a massive surge of attention.

The game World of Warcraft and universes such as Second Life and Habbo Hotel are among the most popular.

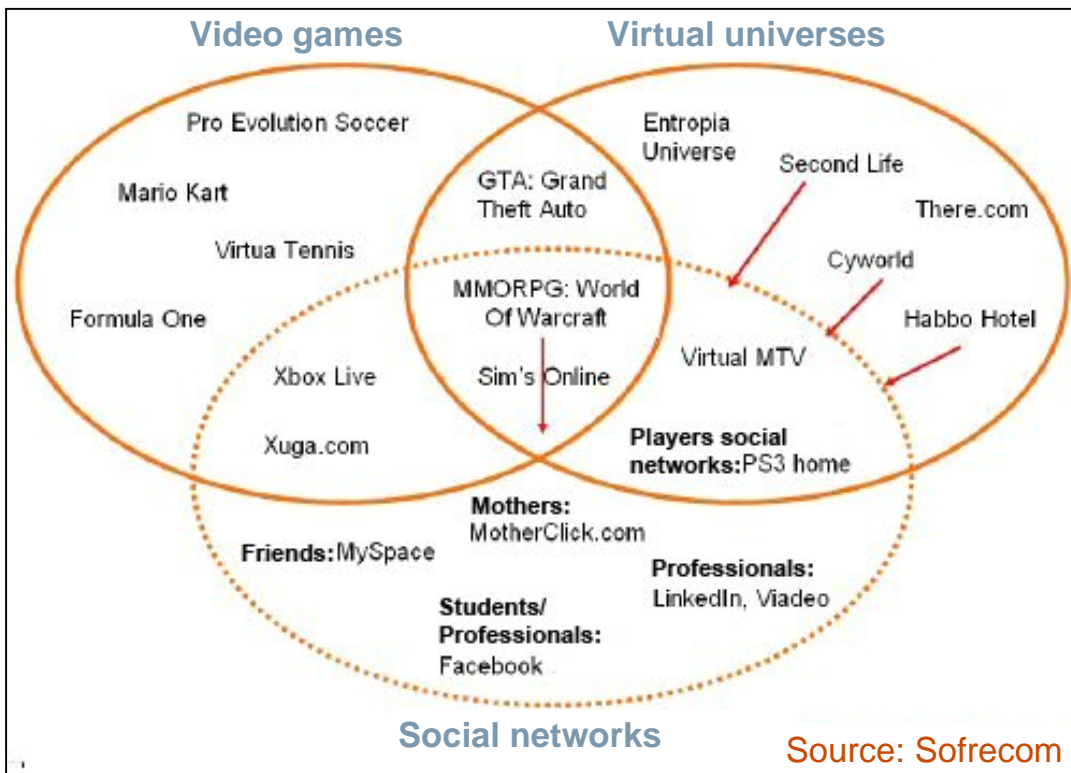


Figure 1: Virtual Worlds and Associated Universes [1]

These ever-expanding universes are persistent worlds populated by avatars. These are the virtual representations of those who frequent them. They can change physical appearance and clothing as they wish. In many cases, these are players, as the majority of these worlds are game spaces. They are known as MMORPG: Massive Multiplayer Online Role-Playing Games, and are often mythical universes where heroes, warriors, magic, sorcery, ancient cultures and supernatural elements coexist. For the most part, I qualify them as medieval (i.e., fantasy), unlike futuristic places like Entropia Universe.

For those who do not wish to risk their life at every crossing and who simply wish to meet people and gather around various centers of interest, there are several universes aside. These are social universes like Second Life.

¹ Virtual worlds: Waiting for Metaverse: http://stephanebayle.typepad.com/sl_business_review/Orange-Metaverse.pdf

Name of Game	Category
Dofus Final Fantasy XI Guild Wars Knight Online Lineage Lineage II Runescape World of Warcraft	Fantasy Role Playing
Entropia Universe	Sci-Fi Role Playing
Second Life	Social

Table 1: The top 10 virtual universes

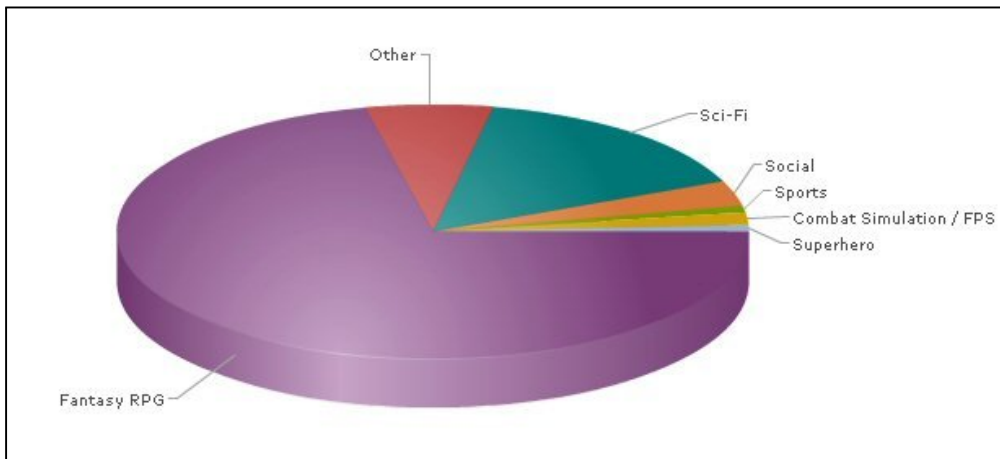


Figure 2: MMORPG by Genre

Gartner predicts that, by 2011, 80% of active Internet users [²] could have a second life in a virtual universe [³]. According to estimates, this could represent nearly 60 million virtual residents. This is a reasonable estimate when we consider that there are 7 million users of Habbo Hotel, 8.5 million users of World of Warcraft, 20 million Cyworld customers, and 120 million MySpace accounts. By 2011, China alone could be home to nearly 26 million residents of virtual worlds [⁴].

² An active Internet user is an Internet user who goes beyond merely viewing the Web, who participates in one way or another in its construction: writing a blog, writing comments, participating in a social network / discussion forum, posting videos and other multimedia files online, etc.

³ Gartner Says 80 Percent of Active Internet Users Will Have A "Second Life" in the Virtual World by the End of 2011 : <http://www.gartner.com/it/page.jsp?id=503861>

⁴ Virtual World Population: 50 million by 2011: <http://gigagamez.com/2007/05/24/virtual-world-population-50-million-by-2011/>

Access is free, although limited, for some of them. This is the case with Second Life, where without a subscription, you can move around and make friends, but not buy land or open a business. Others require a monthly subscription. This is the case with World of Warcraft. To differentiate these access styles, experts use the following terminology:

- F2P (Free to Play): totally free,
- B2P (Buy the game to Play): the game is restrained in its free version,
- P2P (Pay to Play): totally paying.

There are more than 8 million active paying accounts in World of Warcraft. Second Life claims to have 6.5 million open accounts, not all of which are necessarily active. Only one hundred thousand of them are premium; that are paying accounts.

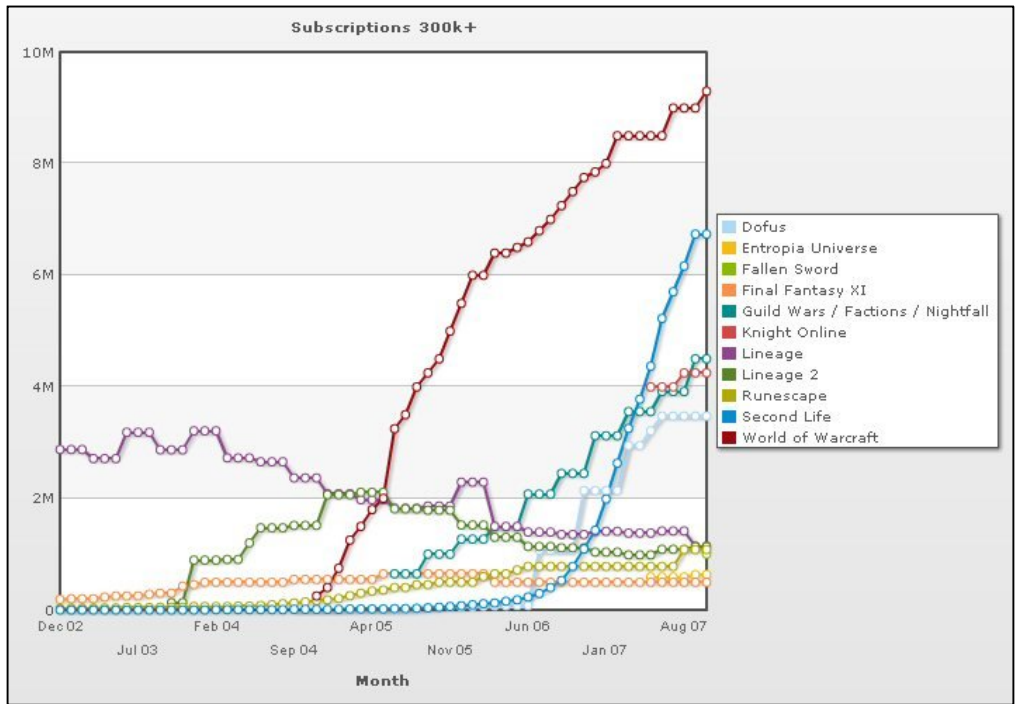


Figure 3: MMORPG by Subscription Number

All of these universes use their own virtual money, which has an exchange rate against euros and dollars.

Game	Associated Money
Dofus	Kamas
Entropia Universe	PED
Final Fantasy XI	Gil
Guild Wars	Gold
Knight Online	Dollars US
Lineage II	Adena
Runescape	Gold
Second Life	Linden Dollar
World of Warcraft	Gold

Table 2: Some money used in virtual worlds

Whatever the chosen world, nothing is possible without money. In Second Life, the brand war is raging. Nike and Adidas are selling shoes. Pontiac and Toyota are selling cars. Security agents, sandwich board men and escort-girls are paid. An exotic dancer pays 20% of their income to their boss. Besides the major names in fashion, all regular users are trying to make a profit by selling necklaces, clothing and other accessories for licentious activities. More than \$1.5 million changes hands each day in Second Life.

On eBay, people bid for characters or virtual objects. "Zeuzo", a WoW "night elf rogue" character was recently sold for 7,000 euros. According to specialists, it was in possession of an exceptionally rare weapon: the Warglaives of Azzinoth, one of only two available in the world [⁵].

In Second Life, trade is not limited to virtual objects. Many individuals and business are buying land.

Outside Threats

Money beckons maliciousness! Even if it bears a different name in each of these universes, the term "gold" in conversations commonly refers to the various types of money that could be encountered. In this second part, we will see that many techniques often used on the Internet for the purpose of financial fraud may also target an avatar and their virtual money.

Gold Keylogging: Trojan

Many keyloggers and password stealers are gaining interest in virtual worlds. They represent perhaps 20 to 30% of all the 85,000 PWS that I recently identified. A majority is detected by VirusScan under generic terms, but some large families are more finely classified. For example:

- PWS-Banker: bank connections
- PWS-MMORPG: various MMORPG games
- PWS-LDPinch: gathers information about the system hosting it. Seeks passwords stored on the disk (ICQ, TheBat, dialup connection, etc.)
- PWS-Lineage: "Lineage" games
- PWS-Legmir: "Legend of Mir" games
- Keylog-Ardamax: captures keystrokes
- PWS-Goldun: "e-gold" accounts (digital currency)
- PWS-WoW: "World of Warcraft" games
- PWS-Gamania: Taiwanese online game site
- PWS-QQGame, QQPass, QQRob: Tecent QQ instant messaging (Asia)

For the top six of them, the following figure shows their change in number over the year 2007.

⁵ The high cost of playing Warcraft: <http://news.bbc.co.uk/2/hi/technology/7007026.stm>

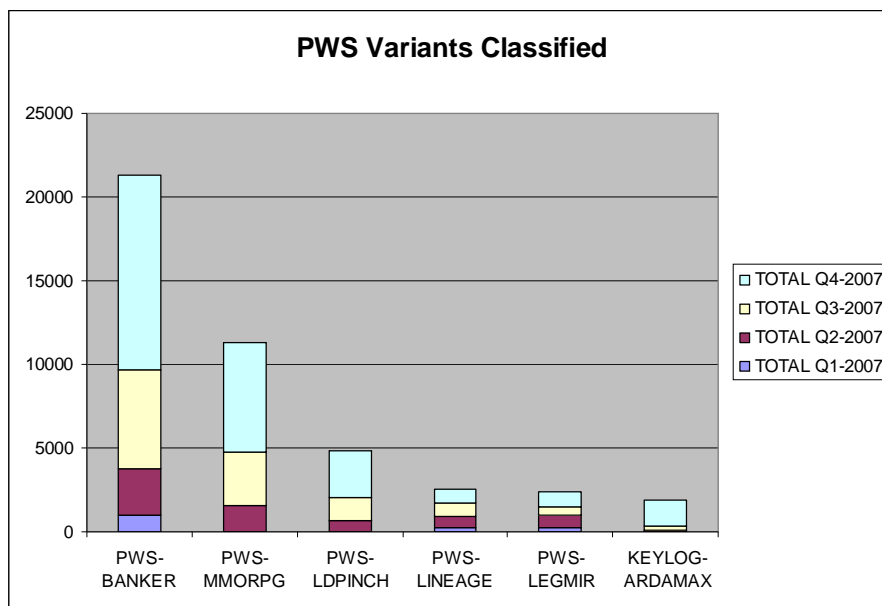


Figure 4: Top PWS names in VirusScan and their evolution over the year 2007

Gold Keylogging: Viruses

Parasitic viruses remain more discreet than Trojans, but most of the newcomers target online games. As shown in the table below, there were many variants of two families of viruses in 2007. They were regularly encountered in the wild, primarily in Southeast Asia.

Virus Name	Number of variants over the period		
	2005	2006	2007
W32/HLLP.Philis	18	158	383
W32/Fujacks	0	11	518

Table 3: The most popular parasitic malware in 2007 (cumulative)

Like W32/Bacalid and W32/Detnat, these 2 viruses are targeting MMORPGs and have payloads related to online gaming.

- **W32/HLLP.Philis** [6]: a prepending virus. Appearing in early 2004, it is written in Delphi and downloaded malware that stole login details for “Lineage” and “Legend of Mir” games.
- **W32/Fujacks** [7]: In 2006 we saw a wave of viruses from that family that targeted “Lineage”, “Legend of Mir” games and the popular Chinese MMORPG game “Zhengtu”. We have to note here that the members of W32/Fujacks family have significant code similarities with W32/HLLP.Philis. The change in classification is due to the modifications in the replication mechanisms—so much so that both families could, in principle, be merged for the purpose of counting. W32/Fujacks started using “Autorun.inf” and modifying HTM and ASP files.

⁶ W32/Philis: http://vil.nai.com/vil/content/v_140403.htm

⁷ W32/Fujacks: http://www.trendmicro.com/vinfo/secadvisories/default6.asp?VNAME=PE_FUJACKS%3A+Jacking+Up+to+the+Times&Page

Phishing

Bank-related phishing also has an equivalent: gold phishing.

In early November, a young Dutch man was arrested for stealing virtual furniture. Using a mirror site, he and 5 other friends are said to have stolen up to 4,000€ worth of e-furniture purchased by their owners in exchange for real money.

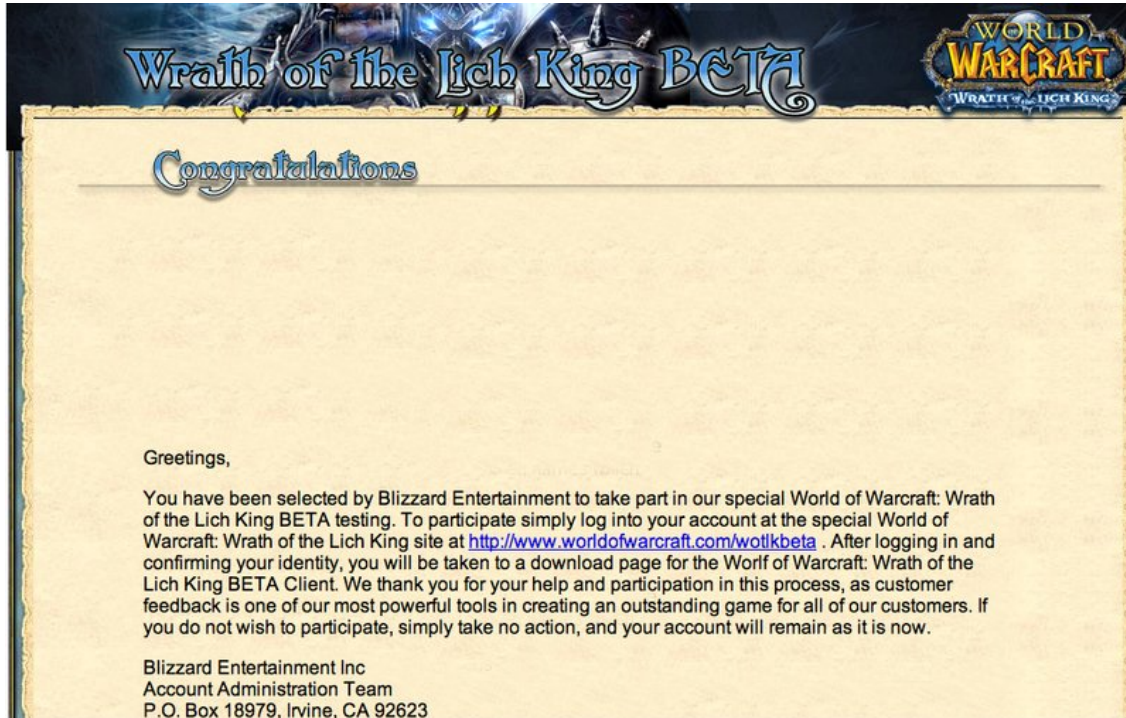


Figure 5: An example of Gold Phishing [8]

The screen capture above is a copy of an e-mail message received by WoW players in October 2007. Believing they were connecting via the provided link, they were in fact redirected to a mirror site resembling a Blizzard site. They were asked for the player's connection info as well as their CD key!

Parallel Financial Networks, the Sex Industry and Extremism

The media regularly reports on reprehensible practices in World of Warcraft and Second Life. This chapter presents some examples. Note, however, that I am not reducing the entire population of these universes to evil beings, criminals or sexual obsessives; this would disrespect the many users who create content and offer friendly places of discussion that are conducive to many exchanges.

Gold Farming

Stories about gold farming aren't new. Linked to certain games like World of Warcraft, it is a new form of modern slavery. Teenagers are exploited in several countries in Southeast Asia. They make virtual money for their employers who re-sell the money for a greater profit. On June 2007, in the New York Times magazine, Julian Dibbel describes his tour of the "gold farms" in China. There, young Chinese men toil over their keyboards for 12 hours a day collecting virtual money in games like World of Warcraft, sleeping in cramped dormitories and earning the equivalent of about 25 cents an hour.

⁸ Source: <http://exodus.superforum.fr/news-f11/warning-keylogger-t2056.htm>

I encourage you to watch this video from the following link:

<http://www.mathewingram.com/work/2007/06/17/new-york-times-portrait-of-a-virtual-sweatshop/>

On the other end of the spectrum, various companies, including the omnipresent IGE, are often pointed at. Antonio Hernandez, an American player from the state of Florida, wishing to represent all World of Warcraft players, recently filed a complaint against this virtual gold dealer. In the official document accompanying the complaint [⁹], the player accuses IGE of making basic resources (minerals, herbs, etc.) rare via gold farming and spamming chat channels. The claimant also alleges that IGE's actions make arena competitions unfair (game field where two teams can battle one another) by reducing the opportunities for honest subscribers to receive rewards (for example, exceptionally strong weapons or armor). According to the complaint, it alleges that IGE's various actions lead to the devaluation of players' virtual money, which results in an economic loss in real dollars.

Gaming Bots

Illegally buying gold and equipment can help a resident to move up the ladder and attain notoriety or a level of game play that only a minority of players reach. It may therefore be tempting to keep an account running 24/7 to allow its owner to accumulate money, objects and experience without having to be physically present in front of the screen. A robot is then used to simulate a human player.

In 2004, Blizzard made the following statement [¹⁰]:

We were recently able to confirm that some people are using third-party robot programs (or "bots") to automate their characters' actions in World of Warcraft. The use of robot programs is in violation with the Terms of Use of World of Warcraft and is therefore strictly prohibited. Consequently, accounts that have been identified as having used robots have been banned.

Blizzard Entertainment considers it to be a priority to maintain a fair game-playing environment in World of Warcraft. As we have said before, our company applies a zero-tolerance policy for all forms of cheating. Players caught using robots to automate actions on behalf of their characters will find their characters deleted and their accounts banned. They will not receive any warning. More than 300 accounts have already been banned for such offences.

Since that date, the statements have continued. Robots are still prohibited, and accounts continue to be deleted without curbing the phenomenon. 500,000 accounts are said to have been suspended between 2004 and April 2006. For example:

- 59,000 accounts deleted in July 2006 [¹¹]
- 114,000 accounts deleted in May 2007 [¹²]

Note that there are many other types of robots, including "poker bots" that give an individual the ability to participate in several games simultaneously and always optimally.

⁹ Hernandez v. IGE : <http://docs.justia.com/cases/federal/district-courts/florida/flsdce/1:2007cv21403/296927/20/0.pdf>

¹⁰ 10/12/04 : Wow Blizzard Zéro Tolérance (Blizzard WoW Zero Tolerance) : http://www.news-hs.com/Wow_Blizzard_Zro_Tolrance-130.html

¹¹ Blizzard bans 59,000 World of Warcraft accounts: <http://nylatenite.wordpress.com/2006/07/27/blizzard-bans-59000-world-of-warcraft-accounts/>

¹² Blizzard bans 114,000 WoW accounts: <http://wow-guides.co.uk/news/blizzard-bans-114000-wow-accounts/>

Sex and Pedophilia

Earning money is one of the main concerns that residents have. Sex is without doubt one of the top activities in Second Life. The encounters, which are often paid for, are far from being the only sources of income. When someone creates an avatar, their features and clothing define their sex. However, they are missing certain “other attributes” that you can, of course, buy. Some providers of sexual positions and naughty accessories earn lots of money: some tens of thousands of dollars per month.

Reflecting our real world, virtual pedophilia is present. Residents who so desire can attempt to have a sexual experience with virtual children. This deviance, which among other things involves using a child avatar in Second Life, is called Ageplay.

Sky News has a video on the subject, available from the following link:

<http://news.sky.com/skynews/article/0,,91221-1290719,00.html>

Extremist Movements

Many extremist or racist groups have websites, so it is not surprising to come across some of them in Second Life. If they do not stay quiet, it seems however that they have trouble remaining there. In December 2006 and with many statements to that effect, the Front National boasted about being "the first French and European political party to establish an official, permanent presence on Second Life"^[13]. The (virtual) demonstrations and signage seem to have very quickly discouraged the followers of this French political group.

Second Life also hosts groups of virtual revolutionaries who try to disturb some islands or properties belonging to leading brands or official political parties. They claim some right of inspection for the avatars on Second Life developments and a form of avatarian democracy that could counterbalance the power of companies, which they believe to be too large with Linden Lab. To distribute their message, they don't hesitate to develop destructive scripts^[14] or call upon hit men. If you have a good understanding of the programming language, you could effectively simulate an attack or kill an avatar. But rest assured, if you are killed in Second Life, you just close the session and re-open it by selecting a calmer location for your next teleport.

¹³ Le Front dans Second Life (The Front in Second Life): <http://e-patriote.spaces.live.com/blog/cns!3265B2FCB3A8C72F!847.entry>

¹⁴ Vandals 'bomb' ABC Island : <http://www.smh.com.au/news/web/vandals-bomb-abc-island/2007/05/22/1179601400256.html>

Inside Threats and Script Languages

Virtual worlds have their own scripting languages. First is “Lua”, because it is common and because it is used in “World of Warcraft”. Second is “LSL” because it is a very rich scripting language of “Second Life” and this environment offers enormous flexibility in supporting commerce, advertising and creativity. Therefore we should expect many standard attacks (phishing, spam, viruses, etc.) to materialize there first.

Until now, we only know some anecdotal facts:

- In 2005, a bug led to a viral epidemic. A deadly and "true virtual pathogenic virus" exterminated characters below level 50. The origin seemed to be related to the application of a patch that put a new dungeon online. In this dungeon players, coders on the side in their spare time, seemed to have "hijacked" a combat spell "Corrupted Blood" by transforming it into a highly communicable item. The developers create "quarantine areas" in which players settled for dying without contaminating "healthy" people.
- In 2006, Second Life temporarily closed its doors following the appearance of a piece of "malicious software". It's a golden ring that splits into two once it is touched. Within a short amount of time, the servers were considerably slow.
- In August 2006, some script viruses which were targeting the Lua script language were discovered by “Garry’s Mod” players. Since this date, various viruses and fake anti-viruses have been circulating in these environments.

LSL Scripting Language

The Linden Scripting Language was developed to allow players create their own objects and define their behavior thus giving users the tools to create the scripts that essentially define local game rules. This exceptional flexibility makes LSL very interesting from security perspective.

LSL is an event-driven C-like language that gets compiled into byte-code and executed in a virtual machine on “Second Life” server. There is no explicit persistency but scripts can be attached to in-game objects (to be precise, scripts are attached to so-called “prims” many of which can be linked into an object) which can be saved and reused.

A tradition in learning programming languages is to start with a very simple program that merely says, "Hello World!" The version adapted for Second Life simply says, "Hello Avatar!" in the chat window. This little program is automatically generated when associating a script to a newly created "prims":

```
default
{
    state_entry()
    {
        llSay(0, "Hello,
Avatar!");
    }
}
```

Figure 6: Example of a basic program in LSL

LSL comes with over 310 built-in functions that allow scripts and objects to interact with their environment. All of the built-in functions start with "ll" -- those are lower-case 'L's, for "Linden Library".

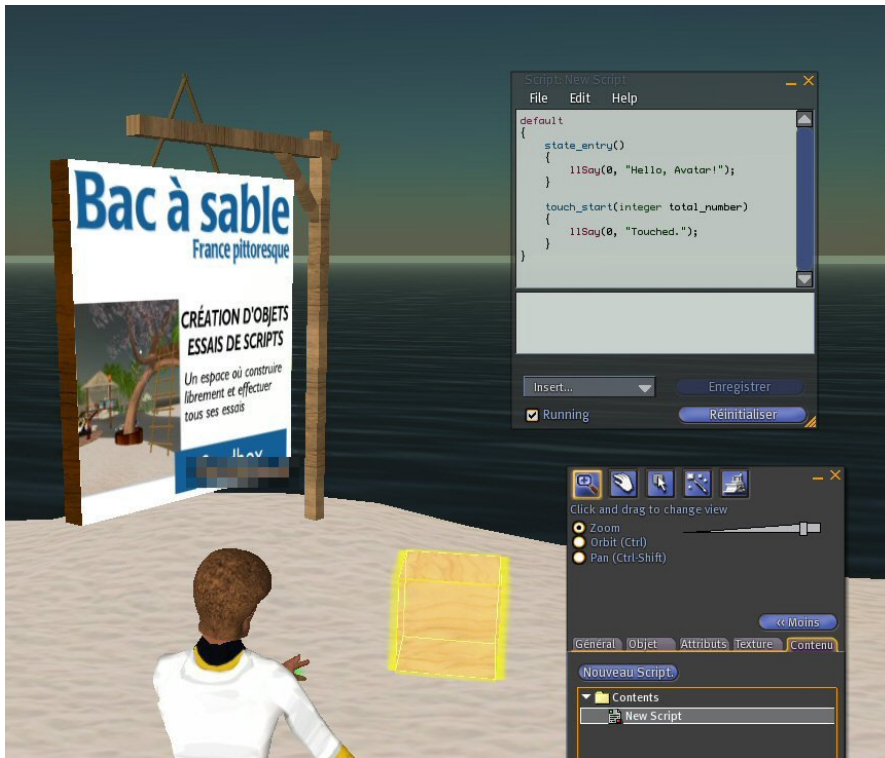


Figure 7: Example of a script in Second Life

With LSL scripting one can create really complex objects and video simulations. With the llParticleSystem function, it is possible to create a visual simulation of a terrorist attack.



Figure 8: Visual effect of a script simulating a big explosion in “Second Life”

Some functions may prove dangerous if they are diverted from their normal use. For example:

- Sending e-mails
 - llEmail. To counter the risk of spam, a 20-second delay is set within the script after sending an email.
- Sending an XML-RPC request
 - llSendRemoteData. To counter the risk of DDoS attacks, a 3-second delay is set within the script after the request.
- HTTP interface
 - llHTTPRequest. 1-second delay
 - llLoadURL. 1-second delay

As mentioned above, for some critical commands, a minimum delay time has been imposed after their execution before the script continues [¹⁵].

Script Delay

Script delay (or just "delay") occurs when either explicitly requested by the developer (scripter) (via `llSleep`) or when certain functions execute built-in delays. The effects of the delay caused by either of these is identical; this page will document these effects.

The functions that automatically delay the script, whether the developer requests it or not, are:

Delay (sec)	Function
20	<code>llEmail</code>
10	<code>llGetSimulatorHostname</code>
10	<code>llLoadURL</code>
5	<code>llTeleportAgentHome</code>
3	<code>llGiveInventory</code>
3	<code>llGiveInventoryList</code>
3	<code>llRemoteDataReply</code>
3	<code>llRemoteLoadScript</code>
3	<code>llRemoteLoadScriptPin</code>
3	<code>llSendRemoteData</code>
2	<code>llInstantMessage</code>
2	<code>llParcelMediaCommandList</code>
2	<code>llParcelMediaQuery</code>
2	<code>llSetParcelMusicURL</code>
1	<code>llCloseRemoteDataChannel</code>
1	<code>llCreateLink</code>
1	<code>llDialog</code>
1	<code>llModPow</code>
1	<code>llOpenRemoteDataChannel</code>
1	<code>llPreloadSound</code>
1	<code>llRequestInventoryData</code>
1	<code>llRequestSimulatorData</code>

Figure 9: LSL Wiki : ScriptDelay

Conclusion

I won't end this document on a negative note. Virtual worlds are true places for exchanges for individuals, artists and businesses as long as they do not lock themselves away in them and forget to go out into the real world.

Here in virtual worlds, however, threats are abundant, and although I haven't fully addressed them in this first version of the document, the reader can still see their great diversity. They first were transposed from the real world to the traditional Internet world. They are now moving to virtual worlds where money circulates in an environment where security has not yet found its place.

Here again, risk management must be a concern across the board, integrating its technical, economic, human and legal dimensions. Among the trails to explore over the next few months are:

- the need for better authentication when connecting to the server,
- consideration for security aspects when developing this type of game software,
- the introduction of a tax (in virtual money) for some types of e-mails or some XML/RPC requests, which could discourage spam and DDoS attacks,
- creation of a virtual police force that could "penalize" offenders,

¹⁵ LSL Wiki : ScriptDelay: <http://lslwiki.net/lslwiki/wakka.php?wakka=ScriptDelay>

- recording the origin of certain potentially dangerous activities and financial transactions surpassing a certain threshold or frequency in centralized log files,
- automated searching for some forms of cheating, associated with automated punishments, such as rollbacks. This will restore the state of the virtual world to some previous historic point (which will revert all modifications that took place after this moment in time, including movement of characters and/or transactions that took place),
- the need to consider a possible legal status for avatars.

We must successfully work together (AV researchers, online game developers and authorities), because we cannot escape the development and infatuation for these new universes that, whatever we think of them, could revolutionize the Internet of tomorrow.

Acknowledgements

Many thanks to Dr. Igor Muttik of Avert Labs. He wrote and presented a paper at the last AVAR conference. I found a great deal of information in his document that helped me to prepare this presentation.