

Jugando sucio

Autor: Cristian Borghello, Technical & Educational Manager de ESET para
Latinoamérica
Fecha: Lunes 14 de julio de 2008



Fantasía no tiene límites...

La historia sin fin, Michael Ende, 1979

...y la cantidad de malware actual tampoco.

La “historia sin fin” parece un reflejo exacto de lo que sucede hoy: el bien y el mal en una “eterna” batalla entre las empresas desarrolladoras de productos antimalware y los creadores de malware.

Esta batalla ahora ha cambiado de terreno y se dirige hacia aquellos campos desconocidos e inexplorados hasta hace poco: los jugadores online (*gamers*), en donde todo es fantasía... y también realidad.

Desde pequeños, siempre nos han incentivado hacia los juegos, porque estimulan nuevas capacidades del ser humano; sin embargo, la nueva generación de juegos en línea del siglo XXI parece desafiar esa regla, estableciendo nuevos peligros, de los cuales sólo uno es mencionado en el presente artículo: la forma en que el malware puede aprovecharse de estos jugadores.

Parece inadmisibles que jugar pueda representar una amenaza pero, lamentablemente, los creadores de malware han encontrado en este fenómeno una nueva forma de hacer dinero, lo que asegura una larga estadía en esta nueva plataforma de ataque.

Fantasías, MMORPG y robos

La historias, literatura y juegos fantásticos han representando desde siempre una de las formas más divertidas de explotar el intelecto humano, y si el juego carece de reglas estrictas, muchísimo mejor. Esto sucedió con la aparición de los juegos de roles [1] en los años '70 en EE.UU. cuando se desarrolla Dungeons & Dragons [2], que termina dando origen a los juegos de rol.

Estos juegos también tienen su forma online y basan su funcionamiento en una conexión cliente (el jugador) y servidor (donde se ejecuta y administra la plataforma del juego). En los primeros tiempos este tipo de juegos carecían de interfaz o la misma era muy precaria dando origen a los MUD (Multi User Dungeon) [3], generalmente basados en texto y que no requerían de herramientas ni software adicionales más que una conexión de terminal (generalmente *telnet* o similar).

Con el tiempo, la evolución natural los llevó a tener una interfaz sumamente avanzada con alta interacción del jugador, dando lugar al nacimiento de los actuales MMORPG (Massive Multiplayer Online Role-Playing Games o Juegos de Rol Multijugador Masivo Online, en español) [4]. Estos juegos permiten interactuar a miles de jugadores de forma simultánea en un mundo virtual a través de Internet, de manera

que se invierte una gran cantidad de tiempo jugando. Según un estudio [5], el 70% de los jugadores invierte más de 10 horas continuas.

Actualmente han surgido los MMOG (Massively Multiplayer Online Game) [6] heredando parte del componente de los MMORPG originales, pero para cualquier plataforma capaz de conectarse a Internet, tales como PlayStation, Xbox, Wii y otras consolas.

Este tipo de juegos se basan en un personaje (avatar) que desarrolla su vida en un entorno propio del juego. Cada avatar es capaz de interactuar con sus pares en distintas aventuras y viéndose recompensado con experiencia social, política y económica, con tesoros, armamento, vestimenta y evolución en aspectos considerados de cada juego en particular.

En resumen, cada avatar (persona virtual) es partícipe de una historia fantástica, en un mundo fantástico que le permite evolucionar en el mundo de fantasía, pero con jugadores (personas físicas) reales, en tiempos reales, con información real y con pérdidas reales (de tiempo, de dinero, del avatar, etc).

A esta información es a la que apuntan los delincuentes, ya que la misma les permitirá obtener dinero tangible en esferas en donde la fantasía deja lugar a las estafas y robos.

Realidad y sumas millonarias

Los juegos sobre plataformas virtuales, se comienzan a popularizar a mediados de los '90 en Asia (principalmente China y Corea) con juegos como The Golden Age, EverQuest y Lineage. Pero la gran explosión se hace en el nuevo siglo cuando aparecen juegos como World of Warcraft (WoW), Dark Age of Camelot, EverQuest, Legend of Mir (LoM), Second Life (basado en el libro de ciencia ficción Snow Crash), Tibia, RuneScape, Habbo y la secuela de Lineage [7].

Actualmente, el mercado de los MMORPG representa un negocio multimillonario [8] en donde cientos de juegos le pelean el lugar a los más conocidos y populares, como WoW que ya ha superado los 10 millones de suscripciones [9] con 62% del mercado y Lineage que ya había superado los 3 millones en mayo de 2007.

Para conocer el escenario de lo que sucede en los juegos se deben tener en cuenta los siguientes puntos:

1. Algunos de estos juegos requieren una registraci3n o suscripci3n paga (llamados VIP) para poder conectarse al servidor. En muchos, se puede jugar gratuitamente y en otros existe la modalidad doble (paga y gratuita) o con acceso limitado.
2. Cada avatar evoluciona y adquiere caracterfsticas que lo hacen tener un valor en s3 mismo.
3. Cada jugador invierte una gran cantidad de tiempo en desarrollar su 3lter ego, que puede ser revendido a otros jugadores que deseen experimentar o jugar con avatares m3s desarrollados o evolucionados.
4. La interacci3n entre jugadores suele requerir la obtenci3n de dinero (u otros bienes) para realizar intercambios, trueques, acuerdos comerciales o simplemente la compra/venta de otros objetos y habilidades propias del juego.
5. El dinero virtual de muchos juegos cotiza en dinero real en el mundo ffsico. Por ejemplo, en Second Life 1 U\$S fluct3a entre los 250 y 275 Lindens (L\$) [10].
6. Si un avatar logra altos niveles de evoluci3n, podr3a tener acceso a una importante cantidad de recursos y dinero.

Es decir que millones de usuarios han encontrado la forma de convertirse virtual y literalmente en "millonarios" y este punto, de por s3, ya es para destacar cuando se habla de su relaci3n con el malware.

Seg3n estimaciones, desde el 2006 la industria de los juegos podr3a crecer a una tasa anual del 95% a lo largo de los pr3ximos cinco a3os, esperando que sea valorado en m3s de U\$S 65 millones para el a3o 2011.

Los juegos hab3an pasado desapercibidos en el pasado para los creadores de malware, pero la alta rentabilidad de los mismos hizo que pusieran sus ojos en este tipo de plataformas, ya que controlando los recursos de los jugadores, se puede controlar el acceso al dinero real invertido en el mundo virtual.

Al igual que con los juegos, el uso de malware para obtener ventajas de este tipo de software comenz3 en Asia en el 2006 (coincidentemente con la explosi3n medi3tica de Second Life) y la mayor3a de los ataques se basan en el mismo principio: el uso de la Ingenier3a Social [11] para obtener las credenciales (usuario, contrase3a y cualquier otro tipo de informaci3n) de los jugadores.

Ya a finales del 2006 y 2007 desde ESET Latinoamérica se advertía acerca de la importancia de comenzar a pensar en la prevención de este tipo de ataques [12], porque habían afectado una masa crítica de jugadores en el continente americano. Esta tendencia quedó de manifiesto en el informe de junio de 2008, en donde puede verse que los troyanos detectados por ESET como *Win32/PSW.OnLineGames* ocupan la primera posición por un amplio margen [13]:

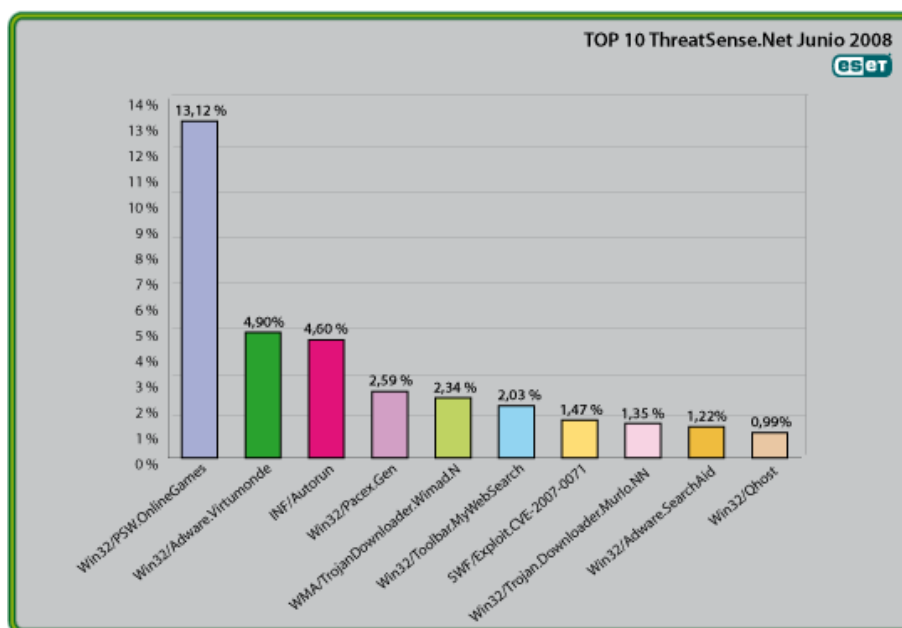


Imagen 2-Ranking de detección de ESET en junio de 2008

Métodos para robar información

La cantidad de metodologías que utiliza el malware para aprovecharse de los juegos MMOG, y por ende de sus usuarios, ha ido evolucionado desde técnicas rudimentarias hasta las actuales más elaboradas, pero todas conservan el mismo objetivo de robar información sensible del usuario para hacerse con el control del avatar y sus características.

Las principales metodologías utilizadas para obtener la información del usuario son las siguientes:

- Instalación de troyanos en el equipo del gamer
- Instalación de Password-Staling (robo de contraseñas)

- Monitoreo de actividades del sistema, esperando que un evento ocurra (por ejemplo, el inicio del juego)
- Instalación de keylogger
- Control de archivos de log del sistema y del juego para obtener información
- Búsqueda de claves del registro y archivos que puedan ser comprometidos
- Intercepción de llamadas al sistema operativo realizadas por el juego
- Utilización de *hooks* para interceptar llamadas del juego
- Monitoreo del tráfico de red para obtener la información transferida entre el servidor del juego y el cliente
- Inyección de código a distintos procesos del sistema.

Una vez que el malware determina que un juego está instalado en el sistema o que el mismo se encuentra activo, comienza a realizar algunas de esas actividades (o combinación de ellas) para obtener la información deseada:

- Nombre de usuario
- Contraseñas
- Datos del servidor utilizado
- En el caso de servidores pagos, información financiera como números de tarjeta, fechas de vencimiento, pin, etc.
- Montos de dinero, evolución, equipamiento, defensa, intelecto, velocidad, cantidad y tipos de objetos, rol, ocupación, nivel del juego, mapas, género, etc.

La información almacenada y obtenida será enviada al delincuente a través de diferentes medios como por ejemplo, un sitio controlado por el atacante (por HTTP Post), un servidor FTP, vía email (a través de un SMTP propio), canales abiertos o cifrados dependiendo del malware que se trate.

La obtención de esta información tiene como objetivo a los juegos más populares y extendidos como WoW, Lineage I y II, LoM y Second Life, pero las similitudes entre los juegos, las formas de registro y los datos necesarios para jugar hacen que el malware ya existente pueda ser modificado fácilmente para adaptarse a otro juego si fuera necesario, dando lugar a miles de diferentes variantes.

Análisis de un caso específico

A continuación, se analizará una variante del malware denominado por ESET como *Win32/PSW.Lineage* desarrollado específicamente para el juego Lineage II, Chronicle 4.

Este programa dañino es un troyano con capacidades de keylogger y rootkit [14] que utiliza sitios web, las redes P2P, el correo electrónico o los dispositivos removibles como llaves USB y memorias flash, para propagarse.

Una vez que el malware se ha descargado en el sistema y es ejecutado, oculta sus actividades al sistema y controla el momento en que se inicia el juego mencionado y se solicitan las credenciales del usuario:



Imagen 3-Solicitud de credenciales por parte de Lineage II

Al utilizar capacidad de rootkit, los procesos del malware no son visualizados por el sistema y tampoco por el usuario. Utilizando ESET SysInspector [15] pueden encontrarse en el directorio X:\windows\system32 (donde X:\ es la unidad del sistema) a los ejecutables encargados del keylogging:

keydll.dll	33 KB
Verkey.exe	53 KB

Imagen 4-Archivos del malware encargados de keylogging

Los archivos keydll.dll y Verkey.exe son detectados por heurística por ESET NOD32 como *probably a variant of Win32/PSW.Lineage* y son inyectados en diferentes procesos del sistema para controlar las acciones del usuario. A continuación, se muestra esta situación a través de ESET SysInspector [15]:

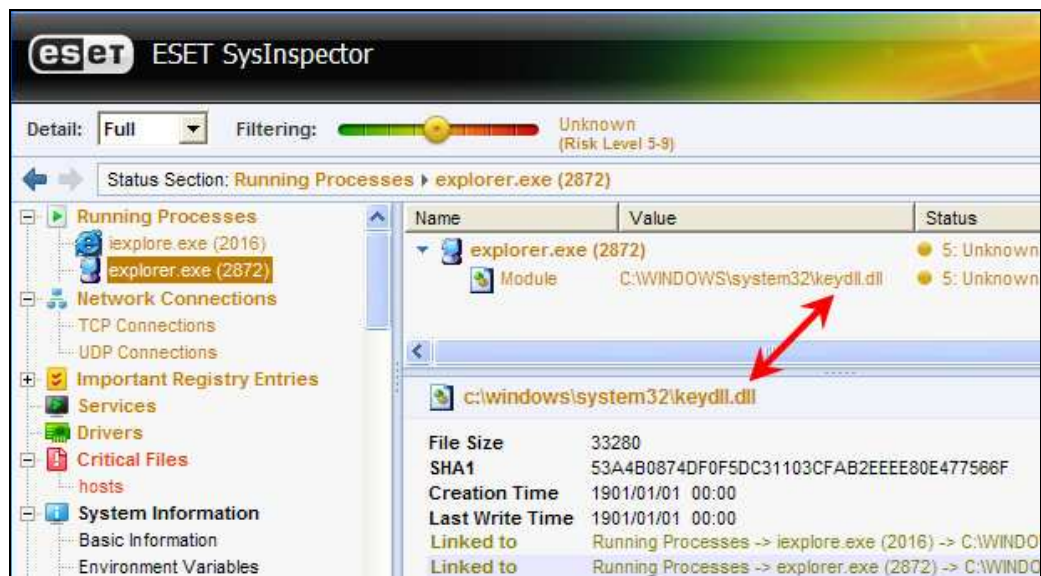


Imagen 5-Detección de procesos inyectados por ESET SysInspector

A partir de ese momento, el keylogger graba las teclas presionadas por el usuario y las almacena en un archivo en el disco raíz del sistema operativo:

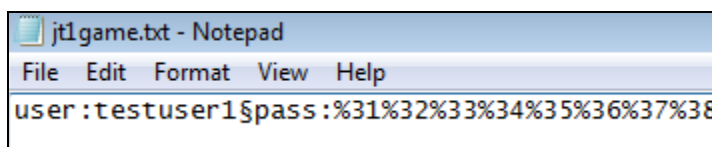


Imagen 6-Datos grabados por el troyano

En este caso, los datos almacenados corresponden al nombre de usuario y contraseña (ofuscada en hexadecimal).

Nota: Si se desea ver el funcionamiento detallado de este malware es recomendable ver el video educativo que ESET Latinoamérica ha preparado sobre este caso [16].

Detección y protección

La cantidad de variantes actuales de este malware asciende a miles y aparecen nuevas versiones cada minuto, lo que convierte en inútil cualquier intento de analizar y describir cada uno de ellos, teniendo que optar por las detecciones genéricas y utilizando heurística para su detección:



Imagen 7-Detección heurística del malware Win32/PSW.Lineage

Con respecto a la prevención de este tipo de malware, son las mismas que para cualquier otra amenaza debido a que, según lo expuesto, los medios de propagación utilizados pueden ser cualquiera.

- Utilizar un antivirus con capacidades de detección proactiva
- No desactivar el antivirus al utilizar juegos que consuman muchos recursos. Es necesario buscar la solución ideal que permita utilizar juegos de este tipo sin la necesidad de desactivar la protección contra el malware.
- No descargar archivos de fuentes dudosas
- Explorar con el antivirus cualquier archivo descargado, antes de ejecutarlo
- Inspeccionar las unidades removibles
- Verificar los correos recibidos para asegurarse que son reales

Considerando las características de este tipo de malware y su orientación hacia los juegos online, los jugadores deberían tener en cuenta las siguientes recomendaciones, además de las anteriores:

- Utilizar servidores de juegos de confianza
- Descargar actualizaciones mods, hacks, cheats y otras herramientas de terceras partes de servidores oficiales o de confianza

- Utilizar contraseñas fuertes para evitar ataques de fuerza bruta sobre la misma
- No ingresar información confidencial del jugador o del avatar en foros, listas de correos, etc.
- Visitar los sitios oficiales de cada juego para conocer las recomendaciones en cada caso. Leer la licencia (EULA, End User License Agreement) de cada juego para conocer lo que está permitido o prohibido en cada juego.
 - Algunos juegos disponen de aplicaciones que permiten la detección de programas dañinos desarrollados para esos juegos en particular (Anti-Cheat, GameGuard, PunkBuster, Blizzard Launcher y otros).
 - Prestar atención a los correos electrónicos recibidos masivamente (spam) con intentos de phishing u ofreciendo “ventajas” a los jugadores. Este tipo de correos suelen ser anzuelos para robar información o instalar programas dañinos en el sistema.

Conclusiones

Los creadores de malware son personas que conocen perfectamente el mercado y apuntan sus creaciones a aquellos lugares en donde saben que pueden maximizar sus ganancias.

Actualmente, cualquier actividad (desde el trabajo al ocio) puede ser llevada a cabo en Internet y si el sistema no es controlado y utilizado responsablemente, adoptando las medidas de seguridad adecuadas, estas actividades se pueden ver seriamente afectadas.

La cantidad de jugadores online y la posibilidad de intercambio de objetos entre el mundo virtual y el real ofrecen la posibilidad de que estos tengan un valor suficientemente importante para que los mismos deseen ser obtenidos por delincuentes. Además, y como siempre, el tráfico de información sensible ya tiene de por sí el suficiente valor monetario en los mercados en los que se mueven estos personajes.

Como las plataformas de juego son diversas, es de esperar que estas amenazas se comiencen a desarrollar para cualquier sistema operativo y plataforma.

En este recorrido por los juegos online y sus amenazas se deja en claro que este tipo de juegos de rol representan un negocio millonario y que por eso los jugadores en línea tienen mucho que perder, por lo que tomar las medidas adecuadas es, una vez más, responsabilidad de cada usuario.

Epílogo

Este documento destaca la importancia de la protección en el caso de ser jugador, pero el malware orientado a los juegos en línea, al copiarse al sistema, no verifican (ni tienen posibilidad de hacerlo) si el dueño del sistema es un gamer o no, por lo que lo infectará sin más.

Es decir que el usuario estará infectado sin importar si alguna vez jugó, y será utilizado como un medio de infección hacia otros usuarios a través de los canales ya comentados. Es por eso que si bien puede pensarse que en Latinoamérica la cantidad de jugadores no es la misma que en Asia, la tasa de propagación mostrada en la imagen 2 es excesivamente alta.

Como conclusión cabe destacar entonces que este tipo de malware no es una fantasía y no se circunscriben a los jugadores, sino que es un problema de todos los usuarios de Internet y es por eso que es necesario tomar las medidas necesarias.

Más información:

[1] Juego de rol

http://es.wikipedia.org/wiki/Juego_de_rol

[2] Juego Dungeons & Dragons

[http://es.wikipedia.org/wiki/Dungeons_%26_Dragons_\(juego_de_rol\)](http://es.wikipedia.org/wiki/Dungeons_%26_Dragons_(juego_de_rol))

[3] MUD

<http://es.wikipedia.org/wiki/MUD>

[4] MMORPGs

<http://es.wikipedia.org/wiki/MMORPG>

<http://iml.jou.ufl.edu/projects/Spring05/Hill/mmorpg.html>

[5] The Psychology of Massively Multi-User Online Role-Playing Games

[http://www.nickyee.com/pubs/Yee%20-%20MMORPG%20Psychology%20\(2006\).pdf](http://www.nickyee.com/pubs/Yee%20-%20MMORPG%20Psychology%20(2006).pdf)

[6] MMOG

<http://es.wikipedia.org/wiki/MMOG>

<http://archive.gamespy.com/amdmog/week1/>

[7] An Analysis of MMOG Subscription Growth

<http://www.mmogchart.com/analysis-and-conclusions/>

<http://iml.jou.ufl.edu/projects/Spring05/Hill/mmorpg.html>

[8] Los juegos virtuales en la Red mueven 900 millones de dólares al año

<http://www.laflecha.net/canales/videojuegos/los-juegos-virtuales-en-la-red-mueven-900-millones-de-dolares-al-año/>

[9] MMOG Active Subscriptions

<http://www.mmogchart.com/charts/>

[10] Cotización de Lindes L\$

<http://blog.secondlife.com/?s=exchange>

<http://blog.secondlife.com/2007/01/04/l-exchange-data-update/>

<http://www.rankia.com/blog/familyoffice/2007/06/second-life-inversin-para-real-life.html>

[11] Ingeniería Social

<http://www.eset-la.com/threat-center/1515-arma-infalible-ingenieria-social>

[12] Tendencias del malware 2007 y 2008

<http://www.eset-la.com/threat-center/1538--tendencias-del-malware-para-2007>

<http://www.eset-la.com/threat-center/1709-tendencias-2008>

[13] Ranking de Propagación de Junio

<http://www.eset-la.com/company/1776-ranking-virus-eset-junio-2008>

[14] Rootkits, jugando a las escondidas

<http://www.eset-la.com/threat-center/1755-080429-analisis-tecnico-eset-rootkits>

[15] ESET SysInspector

<http://www.eset-la.com/sysinspector>

[16] Videos Educativos de ESET Latinoamérica

<http://www.eset-la.com/threat-center/videos/>

Plataforma Educativa de ESET Latinoamérica

<http://edu.eset-la.com>

Blog de Laboratorio de ESET Latinoamérica

<http://blogs.eset-la.com/laboratorio>