Jugando con desconocidos

Jugando sucio

Fantasía no tiene límites…
La historia sin fín, 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 los creadores de malware y las empresas desarrolladoras de productos antimalware.

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

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

Parece inadmisible 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

Las historias, literatura y juegos fantásticos han representando desde siempre una de las forma más divertidas de explotar el intelecto humano y si el juego carece de reglas, 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], quien termina dando origen a los juegos de rol.

Estos juegos 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 interface o la misma era muy precaria dando origen a los MUD (Multi User Dungeon) [3], generalmente basado 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 llevo a tener una interface 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] permitiendo interactuar a miles de jugadores de forma simultánea en un mundo virtual a través de Internet, invirtiendo en ello gran cantidad de tiempo jugando (el 70% de los jugadores invierte más de 10 horas continuas según un estudio) [5].

Luego 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 y Wii.
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 en cada juego en particular.

En resumen, cada avatar (persona virtual) es partícipe de una historia fantástica, en un mundo fantástico que le permite obtener niveles de evolución fantástica, pero con jugadores (personas físicas) reales, en tiempos reales, con información real y con dinero real.

A esta información es a quien 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 comienza 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 debe tener en cuenta los siguientes puntos:

1. Muchos de estos juegos requieren una registración o suscripción 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 limitada en el caso de ser gratuita.
2. Cada jugador invierte una gran cantidad de tiempo en desarrollar su álter ego y el mismo puede ser revendido a otros jugadores que deseen experimentar con avatares más desarrollados o evolucionados.
3. Cada avatar evoluciona y adquiere características que lo hacen tener un valor en sí mismo.
4. La interacción entre jugadores suele requerir obtener 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 físico. Por ejemplo en Second Life un U$S fluctúa entre los 250 y 275 Lindens (L$) [11].
6. Si un avatar logra un nivel de evolución importante es obvio que tendrá acceso a una cantidad de recursos y dinero importantes.

Es decir que millones de usuarios han encontrado la forma de convertirse virtual y literalmente en “millonarios” y ese es el punto, de por sí, ya es el importante a destacar cuando se habla de su relación con el malware.
Esta alta rentabilidad de los mismos ha hecho que los creadores de malware pongan sus ojos en este tipo de plataformas ya que, controlando los recursos de los jugadores, pueden controlar el acceso al dinero real de los mismos.

Al igual que con los juegos, el malware para obtener ventajas de este tipo de software comenzó en Asia en 2006 (coincidentemente con la explosión mediática de Second Life) y la mayoría de ellos se basan el mismo principio: el uso de la Ingeniería Social [12] para obtener las credenciales (usuario, contraseña y cualquier otro tipo de información) de los jugadores.

Ya a finales de 2006 y 2007 en ESET Latinoamérica advertíamos sobre la importancia de comenzar a pensar en la prevención de este tipo de ataques [13] porque los mismos ya han adquirido una masa crítica de jugadores en el continente americano.

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-Stealing (robo de contraseñas)
- Monitoreo de actividades del sistema, esperando que un evento ocurra (por ejemplo inicio del juego)
- Instalación de Keylogger
- Control de archives 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 utilizadas por el juego
- Utilización de *hooks* para interceptar llamadas del juego [15]
- Monitoreo de tráfico de red para obtener la información 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 que desee obtener:

- 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 un sitio controlado por el atacante (por HTTP Post), a un servidor FTP, por email (a través de un SMTP propio), por canales abiertos o cifrados dependiendo del malware que se trate.

La obtención de esta información tiene como objetivos a los juegos más populares y extendidos, 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.

Detección y protección

A continuación les damos algunas recomendaciones para las amenazas que existen hoy en día:

- Utilizar un antivirus con capacidades de detección proactiva
- 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 considerar 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 o 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 objetos 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 los 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 uno de nosotros.

Epilogo

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 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 y que cada uno de nosotros debe tomar las medidas del caso.

[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)
[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
[6] MMOG
http://es.wikipedia.org/wiki/MMOG
http://archive.gamespy.com/amdmmog/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-a__o/
[9] MMOG Active Subscriptions
http://www.mmogchart.com/charts/
[10] The Role of the Everyday User in the Evolution of MMORPGs
http://www.driftreality.com/london/mmorpgs.users.pdf
http://www.gamedaily.com/articles/features/videogame-business-to-double-by-2011/68577/?biz=1
[11] 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
[12] Ingeniería Social
http://www.eset-la.com/threat-center/1515-arma-infalible-ingenieria-social
[15] Rootkits, jugando a las escondidas
http://www.eset-la.com/threat-center/1755-080429-analisis-tecnico-eset-rootkits
[16] ESET SysInspector
http://www.eset-la.com/sysinspector
[17] Videos Educativos de ESET Latinoamérica
http://www.eset-la.com/threat-center/videos/