UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

División de Ingeniería Eléctrica

INVESTIGACIÓN

Chipeo: las vulnerabilidades del sistema operativo de las consolas de sexta y séptima generación

Asignatura: Sistemas Operativos

Grupo: 6

Docente: Ing. Gunnar Eyal Wolf Iszaevich

Semestre: 2024-2

Integrantes

Isaías Rosas Meza

Jesús Abner Domínguez Chávez

Saida Mayela Sánchez Calvillo

ÍNDICE

INTRODUCCIÓN

El chipeo, también conocido como modificación o flasheo, es un proceso mediante el cual se altera el software o el hardware de una consola de videojuegos para permitir la ejecución de software no autorizado. Este fenómeno ha sido de particular interés en las consolas de sexta y séptima generación debido a las limitaciones impuestas por los fabricantes y las restricciones en la ejecución de los juegos y aplicaciones.

Las consolas de videojuegos de sexta generación, que incluyen la PlayStation 2, Xbox y Gamecube, presentaban sistemas operativos relativamente primitivos en comparación con las versiones actuales. Estas consolas fueron objeto de numerosos intentos de chipeo debido a su popularidad y a las restricciones impuestas por los fabricantes en la ejecución de juegos piratas, copias de seguridad o software homebrew. Los métodos de chipeo para estas consolas a menudo implican la modificación de hardware, como la instalación de chips mod, o el uso de dispositivos como Action Replay o FreeMcBoot para explotar vulnerabilidades en el sistema y ejecutar código no autorizado.

Por otro lado, las consolas de séptima generación, que incluyen la Xbox 360, PlayStation 3 y Wii, presentaban sistemas operativos más avanzados y medidas de seguridad más sólidas. Sin embargo, esto no impidió que los entusiastas encontrarán formas de chipear estas consolas para ejecutar software no autorizado. Las vulnerabilidades en estas consolas variaban desde exploits en el firmware (tipo de software que proporciona instrucciones específicas para controlar los componentes de hardware de un dispositivo) hasta técnicas de ingeniería inversa para eludir las medidas de seguridad implementadas por los fabricantes.

El chipeo de consolas de sexta y séptima generación ha generado debates sobre la legalidad y la ética de modificar dispositivos electrónicos para eludir las restricciones impuestas por los fabricantes. Si bien algunos defienden el chipeo como una forma de ejercer el control sobre los dispositivos que poseen, otros argumentan que socava los derechos de propiedad intelectual y puede tener consecuencias negativas para la industria del videojuego, como la piratería y las pérdidas económicas para desarrolladores y distribuidores.

DESARROLLO

1. VULNERABILIDADES EN EL SISTEMA OPERATIVO

Las consolas de videojuegos son dispositivos electrónicos altamente sofisticados que ejecutan sistemas operativos especializados diseñados para proporcionar una experiencia de juego fluida y robusta. Sin embargo, como cualquier sistema informático, estas consolas también pueden ser vulnerables a una variedad de amenazas de seguridad que podrían comprometer su integridad, confidencialidad y disponibilidad.

Las vulnerabilidades en los sistemas operativos de las consolas de videojuegos pueden surgir debido a una variedad de factores, que incluyen errores en el diseño o la implementación del software, falta de actualizaciones de seguridad, descuido en la configuración del sistema y técnicas de ingeniería social que engañan a los usuarios para que revelen información sensible.

El "chipeo" de consolas de videojuegos implica la modificación del hardware o del software de la consola para permitir la ejecución de software no autorizado, como copias piratas de juegos o aplicaciones no aprobadas por el fabricante.

VULNERABILIDADES EN EL HARDWARE

Los ataques físicos que implican la manipulación del hardware de una consola de videojuegos pueden incluir técnicas como la soldadura de chips, el puenteo de circuitos, el reemplazo de componentes, entre otros. Estos ataques pueden ser utilizados para modificar la consola con el fin de ejecutar software no autorizado, como copias piratas de juegos o firmware personalizado

VULNERABILIDADES EN EL FIRMWARE

El firmware de una consola de videojuegos es el software de bajo nivel que controla el hardware y proporciona funcionalidades básicas. Estas vulnerabilidades pueden ser explotadas mediante técnicas como la manipulación de datos almacenados en la memoria flash o la corrupción de la firma digital utilizada para verificar la autenticidad del firmware.

Firmware downgrading

El Firmware Downgrading, o degradación del firmware, fue una técnica que aprovechaba las vulnerabilidades en versiones antiguas del firmware de la consola para permitir la ejecución de código no autorizado y, por lo tanto, el chipeo de la consola.

La degradación del firmware implicaba revertir la versión del firmware de la consola a una versión más antigua, que contenía vulnerabilidades conocidas que podían ser explotadas por los hackers. Esto a menudo requería el uso de dispositivos de programación y herramientas especializadas para reescribir el firmware de la consola con una versión específica.

Una vez que se había degradado el firmware a una versión vulnerable, los hackers podían aprovechar las vulnerabilidades conocidas para ejecutar código no autorizado y, eventualmente, instalar un chip mod o aplicar otras modificaciones para chipear la consola por completo.

VULNERABILIDADES EN EL PROCESO DE ARRANQUE SEGURO

Muchas consolas de videojuegos utilizan un proceso de arranque seguro para garantizar que solo se ejecute software firmado digitalmente y autorizado por el fabricante. Sin embargo, algunas consolas pueden tener vulnerabilidades en este proceso que pueden ser aprovechadas para cargar software no autorizado durante el arranque.

Algunas vulnerabilidades comunes en el proceso de arranque son

1) Firmas digitales débiles o comprometidas: Si las claves de firma digital utilizadas para verificar la autenticidad del software durante el proceso de arranque son débiles o han sido comprometidas, un atacante podría generar su propio software firmado digitalmente y hacer que la consola lo ejecute como si fuera legítimo.

2) Errores de programación: Los errores de programación en el código responsable de realizar la verificación de la firma digital durante el proceso de arranque pueden ser aprovechados por los atacantes para corromper la memoria y ejecutar código no autorizado.

EXPLOITS EN JUEGOS

Las vulnerabilidades en los exploits de videojuegos son fallos de seguridad específicos dentro de un juego que pueden ser aprovechados por los jugadores o por hackers con conocimientos técnicos y pueden afectar tanto a los juegos en línea como a los juegos para un solo jugador.

Algunos juegos almacenan datos importantes del juego en el lado del cliente (la consola o el PC del jugador) en lugar de en el servidor del juego. Esto puede abrir la puerta a exploits de modificación de datos, donde los jugadores manipulan los datos del juego para obtener ventajas injustas, como más dinero o recursos en el juego, o para realizar acciones que normalmente no serían posibles dentro del juego. También algunos juegos permiten a los jugadores escribir scripts o macros (exploits de scripting y automatización) para automatizar ciertas acciones dentro del juego. Sin embargo, estos scripts también pueden ser utilizados para realizar acciones no autorizadas o automatizar acciones que otorgan una ventaja injusta sobre otros jugadores. Esto puede incluir la automatización de tareas repetitivas para ganar puntos o recursos más rápidamente, o incluso para realizar acciones que no están destinadas a ser posibles dentro del juego.

EXPLOITS EN LA GESTIÓN DE ARCHIVOS

Estas vulnerabilidades pueden presentarse en varias formas y pueden ser un vector de ataque importante para los hackers que intentan chipear la consola. El sistema de archivos es esencial para la organización y gestión de los datos almacenados en la consola, incluyendo el sistema operativo, los juegos, las aplicaciones y otros archivos importantes.

Estos exploits se basan en errores en la forma en la que el sistema operativo de esta consola gestiona los archivos. Por ejemplo: podían manipularse archivos de configuración o archivos temporales para engañar al SO y ejecutar código arbitrario o si el sistema de archivos de una consola no implementa adecuadamente controles de acceso, esto podría permitir a un usuario leer, escribir o eliminar archivos sensibles o críticos del sistema, lo que podría conducir a la toma de control total de la consola.

BUFFER OVERFLOW

Cuando se escribe más información en un buffer de lo que puede contener, se produce lo que se conoce como desbordamiento de búfer (buffer overflow en inglés). Este es un error común en la programación que ocurre cuando se escribe datos más allá de los límites del buffer asignado en la memoria.

Cuando ocurre un desbordamiento de búfer, los datos adicionales pueden sobrescribir áreas adyacentes de memoria que contienen datos críticos para el funcionamiento del programa o del sistema. Estas áreas de memoria críticas pueden incluir variables importantes, direcciones de retorno de funciones, punteros y otras estructuras de datos esenciales.

El impacto de un desbordamiento de búfer puede variar dependiendo del contexto en el que ocurra. En algunos casos, puede causar que el programa se bloquee o se comporte de manera inesperada. Sin embargo, si un atacante es capaz de descubrir áreas de la memoria del SO que no estaban adecuadamente protegidas contra desbordamientos puede aprovechar esta vulnerabilidad para modificar el flujo de ejecución del programa, ejecutar código arbitrario, sobrescribir áreas de memoria críticas, corromper la memoria, entre otras cosas.

2. CONSOLAS DE SEXTA GENERACIÓN

- **PLAYSTATION 2**

HISTORIA

La PlayStation 2 (PS2) es una de las consolas de videojuegos más influyentes y exitosas en la historia de la industria del entretenimiento electrónico. Fue desarrollada por Sony Computer Entertainment y lanzada al mercado el 4 de marzo de 2000 en Japón, y posteriormente en octubre del mismo año en América del Norte y Europa.

La PlayStation 2, ha sido objeto de una variedad de modificaciones y chipeos a lo largo de los años, lo que ha permitido a los usuarios ampliar sus capacidades más allá de los límites establecidos por el fabricante. Estas modificaciones, fueron en su mayoría realizadas con el objetivo de ejecutar copias de seguridad de juegos y software no autorizado.

VULNERABILIDADES EN SISTEMA OPERATIVO

Una de las formas más comunes de modificar la PlayStation 2 y debido a las vulnerabilidades que se encuentran en su hardware, es mediante el uso de modchips, dispositivos electrónicos que se instalan dentro de la consola y que anulan las protecciones de copia implementadas por Sony. Estos modchips, al interceptar y modificar las señales entre el hardware y el software de la consola, permiten la carga de copias de seguridad desde discos quemados o discos duros externos.

Además de los modchips, existen métodos de modificación de software, conocidos como "softmodding", que aprovechan vulnerabilidades en el sistema para ejecutar software no autorizado sin la necesidad de utilizar un modchip físico.

Un método muy popular fue el uso de herramientas como Swap Magic, que permite ejecutar juegos y aplicaciones no autorizadas sin necesidad de realizar modificaciones permanentes en la consola.

- **XBOX**

HISTORIA.

La Xbox, puesta a la venta en Norteamérica el 15 de noviembre del año 2001, fue la primera consola de videojuegos de sobremesa creada por Microsoft, siendo esta su introducción a dicho mercado y a la llamada “guerra de consolas” liberada en ese momento por las empresas japonesas Sony y Nintendo.

Imagen recuperada de:
https://www.mdtech.news/u/fotografias/m/2022/9/9/f608x342-8490_38213_0.jpg

¿CÓMO FUE HACKEADA LA CONSOLA?

Se tiene que la Xbox, al poseer componentes que son compatibles con una computadora, contaba con un disco duro convencional, es decir, que se podía conectar a una computadora sin problema, lo que permitía hacer ver y modificar todos los datos almacenados.

Aunado a ello, la memoria flash, aquella encargada de manejar los datos más importantes de la consola, no tenía encriptado un archivo que fue dejado por error: la SECRET ROM. Este archivo que pesaba 512 Bytes le permite al programador desencriptar el resto de archivos de la memoria, haciendo el proceso de instalar programas externos mucho más fácil. El joven estudiante del MIT que descubrió esta vulnerabilidad se percató que este archivo ya era obsoleto, pero dedujo que si esta versión seguía dentro de la memoria, el archivo final debía estar en otra parte de la consola. Empleando un aparato que permitía conectar la CPU de la consola con el Nvidia MCPX, pudo leer la información que se enviaban entre sí, logrando interceptar la ubicación real de la SECRET ROM.

- **GAMECUBE**

HISTORIA

El GameCube fue lanzado por Nintendo en 2001 y fue una de las consolas más populares de su generación y un gran competidor destacado de la sexta generación de consolas de videojuegos, siendo competencia directa de la PlayStation 2 de Sony y la Xbox de Microsoft.

Imagen recuperada de:
https://th.bing.com/th/id/R.d06abf9ed6029e11d2d5bdc0c96e7374?rik=2WE2vlimuEqdGA&riu=http%3a%2f%2fnintendookie.files.wordpress.com%2f2011%2f11%2fwikipedia_gamecube_pal1.jpg&ehk=Bv%2fyAYjCBSwLwb6eVUNLQk0eKbpzzyNbE6W5qMEqMNA%3d&risl=&pid=ImgRaw&r=0

Esta consola tuvo varias características que lo hicieron atractivo para ciertos segmentos de jugadores, como por ejemplo: contaba con una impresionante biblioteca de juegos exclusivos desarrollados por Nintendo, incluyendo franquicias como Mario, Zelda, Metroid y Super Smash Bros; sus juegos eran de alta calidad y tenían un enfoque en la diversión ofreciendo experiencias de juego únicas y memorables; era innovador desde el punto de vista del hardware; el precio era muy competitivo y sobre todo el diseño de esta consola era conocida por ser compacta y duradera.

VULNERABILIDADES EN SU SISTEMA OPERATIVO

El sistema operativo del Nintendo GameCube, conocido como "MIOS" (MIcrosoft Operating System), presentaba varias vulnerabilidades que los hackers aprovecharon para chipearlo y ejecutar software no autorizado. Algunas de las principales vulnerabilidades incluían:

a) Buffer overflows: permite poder sobrescribir áreas de memoria críticas, corromper la memoria y ejecutar código no autorizado.

b) Exploits en la gestión de archivos: Esto a menudo requería el uso de dispositivos de almacenamiento externo (como tarjetas de memoria SD o discos ópticos especiales) que pudieran interactuar con el sistema operativo del GameCube

c) Firmware downgrading (degradación del firmware): Al degradar el firmware a una versión más antigua, los hackers podían acceder a vulnerabilidades conocidas en esa versión que permitían la ejecución de código no autorizado. Revertir el firmware a una versión más antigua podía introducir problemas de estabilidad y compatibilidad con ciertos juegos y aplicaciones más recientes que requerían las características de firmware más nuevas. Además, Nintendo a menudo lanzaba actualizaciones de firmware para parchear las vulnerabilidades conocidas, lo que dificulta mantener la consola chipeada de forma permanente utilizando esta técnica.

En conjunto, estas vulnerabilidades permiten a los hackers ampliar las capacidades de la consola más allá de lo que originalmente permitía Nintendo.

3. CONSOLAS DE SÉPTIMA GENERACIÓN

- **PLAYSTATION 3**

HISTORIA

La PlayStation 3 (PS3) es una consola de videojuegos desarrollada por Sony Computer Entertainment. Fue lanzada al mercado en noviembre de 2006 en Japón y en marzo de 2007 en América del Norte y Europa. La PS3 fue la sucesora de la exitosa PlayStation 2 y marcó una importante evolución en la industria de los videojuegos, tanto en términos de hardware como de funcionalidades.

Uno de los aspectos más destacados de la PlayStation 3 fue su potente hardware, que incluía un procesador Cell de IBM, desarrollado en conjunto con Sony y Toshiba, así como una GPU Nvidia RSX. Esto permitió a la consola ofrecer gráficos de alta calidad y un rendimiento general sólido, lo que la convirtió en una plataforma atractiva para desarrolladores y jugadores por igual.

Imagen recuperada de: https://th.bing.com/th/id/OIP.KaTRHgA-VjzZsID13l6fsAAAAA?rs=1&pid=ImgDetMain

CHIPEO DE LA CONSOLA

La PS3 ha sido objeto de una amplia variedad de modificaciones, hackeos y chipeos a lo largo de su vida útil. Estas prácticas, llevadas a cabo por desarrolladores aficionados y hackers apasionados, han abierto nuevas posibilidades para los usuarios de la PS3,

permitiéndoles personalizar su experiencia de juego, ejecutar software no autorizado y explorar capacidades más allá de las intenciones originales del fabricante.

VULNERABILIDADES EN EL FIRMWARE

Una de las formas más comunes de modificar la PS3 es mediante el uso de Custom Firmware (CFW), que reemplaza el firmware oficial de la consola con una versión personalizada. Estos CFW permiten la ejecución de software no autorizado, la instalación de aplicaciones externas y, en algunos casos, copias de seguridad de juegos. El proceso de instalación de un CFW a menudo implica el jailbreak de la consola, que implica evadir las restricciones de seguridad para obtener acceso de administrador y permitir la ejecución de software no oficial. También, se optaba por hacer un downgrade de versión de la consola para permanecer en una versión vulnerable que permita la facilidad de instalación de un CFW.

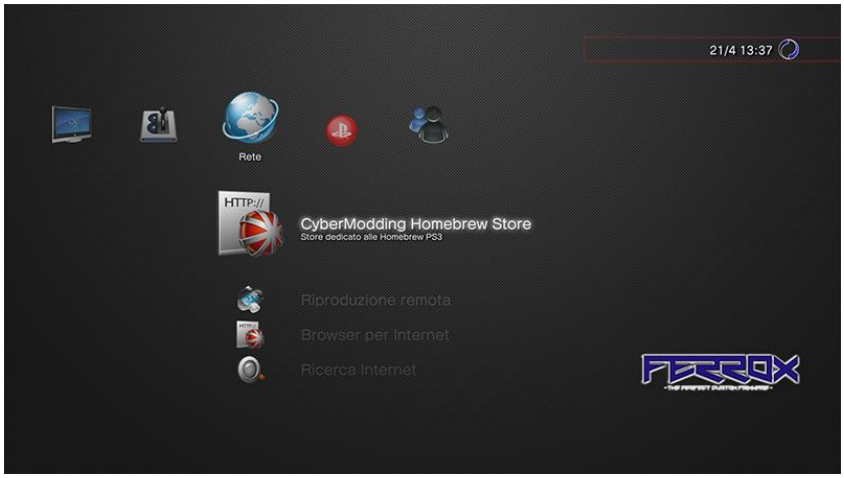

Imagen recuperada de: https://www.psxhax.com/attachments/ps3-cfw-ferrox-4-80-a-png.545/

VULNERABILIDADES EN EL HARDWARE

Además del Custom Firmware, algunos usuarios han optado por instalar modchips en sus PS3. Estos modchips, similares a los mencionados en la PS2, se instalan internamente en la consola y anulan las protecciones de copia implementadas por Sony, lo que permite la carga de copias de seguridad de juegos y la ejecución de software no autorizado.

- **XBOX 360**

ANTECEDENTES

Después de su enorme éxito con el debut del Xbox, Microsoft ahora apuntaba a la creación de una nueva consola de videojuegos que siga el paso de Nintendo y Sony; mejorando los aspectos que funcionaron, corrigiendo los que no, e innovando en otras áreas que brinden una mejor experiencia a sus clientes.

MODIFICACIÓN DEL SOFTWARE

Dentro de los cambios y mejoras que se realizaron estaba la modificación de la placa madre y un nuevo sistema para antipiratería y chipeo al cual llamaron como “Hypervisor”. Este se encargaba de dar permisos y realizar modificaciones sobre el hardware y el sistema de acuerdo a las acciones del usuario. Una de las cosas que podía hacer el Hypervisor era dar permiso de ejecutar un CD si la firma digital que viene incluida en los juegos era confirmada como original por el lector de disco. Es gracias a este detalle que vulnerar la seguridad de la consola en cuanto a hardware fue bastante sencillo, pues con “flashear” el lector de discos se podía engañar al Hypervisor.

Y si bien Microsoft intentó proteger la Xbox 360 cambiando la configuración del lector, haciendo un nuevo lector desde 0, modificando el formato de los discos, implementando revisiones con Wi-Fi, entre otras medidas, todo fue en vano, pues los usuarios lograban vulnerar la seguridad gracias a esa falla del Hypervisor.

MODIFICACIÓN DEL HARDWARE

Para esta nueva generación, Microsoft se encargó de implementar AY Fuses dentro del procesador de la consola, haciendo que cuando la Xbox pase a una nueva versión del sistema uno de estos fusibles se queme. Si el sistema detecta que uno de estos fusibles no se destruyó después de actualizar, la consola se bloqueaba y dejaba de funcionar. Para vulnerar este proceso, se tuvo que modificar otra parte de la consola: el SMC y dos puertos JTAG. Engañando el SMC se podía acceder a dichos puertos para detener el proceso de los AY Fuses y poder manipular las versiones del sistema, donde una de ellas poseía una vulnerabilidad que le permite al hacker instalar distintos softwares.

Pese a los intentos de Microsoft por impedir esto, lo cierto es que todas sus reediciones fueron hackeadas y modificadas siguiendo procedimientos similares, llegando a usar hasta un taladro para destruir un componente sensible del firmware.

- **WII**

HISTORIA

El Nintendo Wii, lanzado en noviembre de 2006, fue un hito en la historia de las consolas de videojuegos. Su nombre en clave durante el desarrollo fue "Revolution", lo que refleja la ambición de Nintendo de revolucionar la forma en que las personas interactúan con los videojuegos.

El Wii se destacó por su innovador controlador inalámbrico, el Wii Remote, que introdujo la detección de movimiento a gran escala en los juegos de consola. Este controlador permitía a los jugadores interactuar de una manera más intuitiva y física con los juegos, atrayendo a una amplia gama de usuarios, incluidos aquellos que tradicionalmente no se consideraban jugadores.

Imagen recuperada de:
https://th.bing.com/th/id/R.b583c205d06f412f38b8cbbfbe845a57?rik=ZET1bRgxC1QyYw&riu=http%3a%2f%2fupload.wikimedia.org%2fwikipedia%2fcommons%2f1%2f14%2fWii-console.jpg&ehk=mp5vIuiod2zwlPTzphn%2bn4klnoGimoNvXgn19yak2kk%3d&risl=&pid=ImgRaw&r=0

VULNERABILIDADES EN SU SISTEMA OPERATIVO

El sistema operativo de la Wii, conocido como "Wii System Menu", es un software desarrollado por Nintendo que proporciona la interfaz de usuario principal de la consola. Este sistema operativo está diseñado para ser fácil de usar y permite a los usuarios acceder a juegos, canales de Wii (aplicaciones preinstaladas y descargables) y configuraciones de la consola.

En cuanto a las vulnerabilidades del sistema operativo de la Wii, hubo varias que los hackers aprovecharon para chipear la consola y ejecutar software no autorizado. Algunas de estas vulnerabilidades incluyeron:

a) Exploits en el canal de juegos: esta vulnerabilidad permite ejecutar código no autorizado a través de canales como la tarjeta SD discos USB o la red

Un exploit popular era LetterBomb. La vulnerabilidad radica en la forma en la que la Wii maneja los mensajes y cómo los interpreta, lo que permitía a los hackers enviar un mensaje especialmente diseñado a una Wii específica. Cuando el usuario abría este mensaje, el código malicioso adjunto al mensaje se ejecutaba automáticamente en la consola. Esto abría una puerta trasera en el sistema que permitía cargar software no autorizado, como el Homebrew Channel, que a su vez permitía ejecutar aplicaciones homebrew y copias de seguridad de juegos. LetterBomb permitía a los usuarios chipear sus consolas sin la necesidad de hardware adicional o modificaciones físicas en la Wii. En lugar de eso, simplemente requería que los usuarios ingresaran la dirección MAC de su Wii en un generador en línea, que luego proporcionaba un archivo "bomb.bin" personalizado que debía copiarse en una tarjeta SD e insertarse en la consola Wii objetivo.

b) Desbordamientos en el buffer:

Cuando se habla de vulnerabilidades en el sistema operativo de la Wii relacionadas con desbordamientos de búfer, significa que los hackers han encontrado formas de aprovechar estos errores de programación para ejecutar código malicioso en la consola y chipearla, lo que permite la ejecución de software no autorizado.

c) Exploits en el boot1 y boot2

El boot1 y el boot2 son componentes del firmware de arranque de la Wii que se ejecutan durante el proceso de encendido de la consola. Los exploits en estos componentes pueden permitir cargar software no autorizado durante el inicio de la Wii. Estos exploits a menudo requieren modificaciones del hardware de la consola para aprovechar las vulnerabilidades en el firmware de arranque, lo que puede implicar soldaduras o cambios físicos en la consola.

CONCLUSIONES

Las vulnerabilidades en el sistema operativo de las consolas han sido una pieza clave en el mundo del hacking y el chipeo, permitiendo a los hackers desarrollar métodos creativos y técnicas innovadoras para desbloquear el potencial de sus dispositivos. Desde exploits en el software del sistema hasta desbordamientos de búfer y modos de arranque alternativos, estas vulnerabilidades han abierto las puertas a un vasto mundo de posibilidades, acceso a características ocultas permitiendo a los usuarios, entre muchas otras cosas, jugar a copias de seguridad de sus juegos sin necesidad de usar los discos originales, lo que puede ser conveniente para preservar los discos originales o para evitar daños por el uso repetido.

Se debe tener en cuenta que la instalación de un chip mod, y en general el chipeo de una consola, puede anular la garantía de esta y dañar su funcionamiento normal. Además, el chipeo para ejecutar copias de seguridad de juegos descargados ilegalmente o infringir los derechos de autor no es compatible con los principios éticos de la comunidad de hacking y modding, aunado a que es ilegal fomentar la piratería de los juegos e infringe con los derechos de autor. Lo que sí está avalado en términos legales es el uso de emuladores, pues estos no buscan atentar contra la integridad de los usuarios y desarrolladores.

Es importante destacar que el descubrimiento y explotación de vulnerabilidades en el sistema operativo de una consola de videojuegos requiere un conocimiento avanzado de seguridad informática y habilidades técnicas especializadas, pues muchos de los componentes que se encuentran dentro del hardware son piezas especializadas y con cierto nivel de encriptación.

FUENTES DE CONSULTA

REFERENCIAS ELECTRÓNICAS

1) https://eloutput.com/videojuegos/reportajes/pirateo-consolas-modelos-mas-vulnerables/

2) https://techstomper.com/ps2-modding-a-history-of-playstation-piracy-part-ii/

3) Microsoft (2015). *Momentos destacados en la historia de Microsoft*. Recuperado el 01 de abril de 2024. Disponible en: https://news.microsoft.com/es-es/2015/04/06/historia-microsoft-40-aniversario/

4) Facu Peralta (2022, 27 nov). *Como TODO EL MUNDO Hackeo la XBOX CLASICA*. Recuperado el 01 de abril de 2024. Disponible en: https://www.youtube.com/watch?v=FbFRHCi8iBs&t

5) Calderón, G. (2021, 2 diciembre). *GameCube | Qué es, características, historia, especificaciones, juegos, modelos*. Euston96. https://www.euston96.com/gamecube/#:~:text=Caracter%C3%ADsticas%20de%20la%20GameCube%201%20Forma%20c%C3%BAbica%20y,juego%20en%20red.%206%20Discos%20de%20juego%20peque%C3%B1os.

6) Facu Peralta (2022, 28 ago). *Como UNA SOLA PERSONA hackeo la XBOX 360*. Recuperado el 01 de abril de 2024. Disponible en: https://www.youtube.com/watch?v=3V5cmMX4dfQ&t

7) Facu Peralta (2022, 30 oct). *Como un TALADRO y KING KONG Hackearon la XBOX 360*. Recuperado el 01 de abril de 2024. Disponible en: https://www.youtube.com/watch?v=am2-vRxK5vU

8) https://pressthepsbutton.wordpress.com/2011/01/26/ps3-jailbreak/

9) https://techstomper.com/ps3-modding-a-history-of-playstation-piracy-part-iii/

10) Colaboradores de Wikipedia. (2024, 27 marzo). *Nintendo GameCube*. Wikipedia, la Enciclopedia Libre. https://es.wikipedia.org/wiki/Nintendo_GameCube