

Problemas de seguridad en sistemas operativos antiguos

Autor: Jorge Mieres, Analista de Seguridad de ESET para Latinoamérica
Fecha: Martes 27 de Enero de 2009

Introducción

Los sistemas operativos Windows 3.x y Windows 9x/ME de Microsoft se ganaron un lugar privilegiado para muchos usuarios, no sólo por su facilidad de uso, sino también por haber iniciado una generación de sistemas que se caracterizaron por el diseño amigable de sus entornos gráficos. Sin embargo a lo largo del tiempo fueron desplazados por versiones evolucionadas.

Entre los puntos más importantes que marcaron la paulatina desaparición de estos sistemas operativos, se encuentran la falta de soporte técnico oficial y de actualizaciones de seguridad por parte de la misma empresa Microsoft, concluyendo así el ciclo de vida de cada uno de ellos. Para una referencia completa sobre los antecedentes históricos de los sistemas operativos de Microsoft por favor **consulte el Anexo**.

En la actualidad, esa falta de soporte ha generado problemas que afectan principalmente a aquellos ambientes informáticos en los cuales se utiliza alguna de las versiones de la familia de plataformas Windows 3.x y Windows 9x/ME, debido a las debilidades y vulnerabilidades que presentan en materia de seguridad.

A través del presente documento se intenta explicar cuáles son los puntos más importantes relacionados con la seguridad que se deben considerar, y por qué los usuarios que aún utilizan alguno de los sistemas operativos antiguos deberían pensar en la posibilidad de migrar hacia nuevas plataformas.

Panorama actual

La constante evolución a nivel tecnológico demanda que para toda nueva tecnología se necesite cumplir con una serie de requisitos con respecto a los programas y dispositivos que se desea implementar.

En este sentido, y teniendo en cuenta que las tecnologías cambian de manera muy rápida y que paralelamente van surgiendo otras, es importante tener presente que esta evolución da lugar a la explotación de nuevas vulnerabilidades.

Pero... ¿cómo afecta esta situación a los sistemas operativos antiguos? Lamentablemente, los problemas con que se ven afectados estos SO son muy importantes.

En julio del 2006, Microsoft decidió dar fin al ciclo de vida de su familia de sistemas operativos Windows 9x/ME y conjuntamente el soporte técnico y actualizaciones (*security updates, update rollups, service packs*) dando esta justificación:

“Microsoft está retirando el soporte para estos productos porque se encuentran desactualizados y pueden exponer a los usuarios a serios riesgos de seguridad. Por lo tanto, Microsoft recomienda que los usuarios que siguen utilizando Windows 98 o Windows Me migren a un nuevo y más seguro sistema operativo lo antes posible”. [9]

Le empresa aconseja, entonces, que se migren los sistemas operativos antiguos hacia sistemas operativos modernos porque estos últimos poseen mejoras en cuanto a las funcionalidades, la productividad y la seguridad de los equipos.

Estas reformas en materia de seguridad forman parte del proyecto iniciado por Microsoft durante el año 2002 denominado “computación confiable” [10] (en inglés, Trustworthy Computing) mediante el cual se pretende mejorar la confiabilidad, la integridad y la disponibilidad de la información.

Sin embargo, todavía existen muchas empresas, entidades gubernamentales y educacionales que utilizan SO antiguos; con lo cual, debido a la falta de soporte oficial y a la falta de parches para la solución de problemas críticos de seguridad, sólo generan importantes y graves problemas al quedar constantemente expuestos a vulnerabilidades antiguas y ataques que vayan surgiendo.

Inconvenientes de seguridad en plataformas antiguas

Antes de comenzar a describir los puntos más sobresalientes que en materia de seguridad presentan los sistemas operativos modernos (Windows 2000, Windows XP, Windows 2003 y Windows Vista) contra los sistemas antiguos (*Legacy System*) representados por Windows 9x/ME y anteriores, es conveniente aclarar qué es el *kernel* de un sistema operativo.

El *kernel* es el núcleo de todo SO, la parte fundamental y más importante de cualquier sistema. Entre sus principales funciones, se encarga de permitir la interacción entre todos y cada uno de los componentes de la PC con los programas gestionando recursos para cada tarea.

La interacción entre los procesos y otros componentes intervinientes en el manejo de recursos del sistema es, en gran medida, quien determina el nivel de seguridad, su rendimiento y el desempeño de las aplicaciones.

En los SO todos los recursos y servicios se ejecutan en determinado nivel de la arquitectura definido por una serie de “anillos” enumerados del 0 al 3 y denominados niveles de privilegio. En plataformas como Windows 9x/ME, las aplicaciones corren en el nivel 0, correspondiente al *kernel*.

En consecuencia, ante el menor de los errores por parte de las aplicaciones y, debido a errores de diseño en la arquitectura, el conjunto de SO antiguos sufren bloqueos y cierres repentinos y las constantes y

conocidas pantallas azules, también conocidas como BSoD (Blue Screen of Death - Pantalla Azul de la Muerte), con lo cual se compromete el rendimiento de las aplicaciones y del sistema mismo perdiendo estabilidad.



Imagen 1 – Ejemplo de Blue Screen of Death

En los sistemas operativos modernos, estos anillos se encuentran dispuestos de manera diferente con respecto a sus antecesores. Las aplicaciones ya no se ejecutan en el núcleo del sistema sino que lo hacen en un nivel con menos privilegios, el nivel 3.

El resultado del cambio en la disposición de los niveles de privilegio, ha permitido disminuir considerablemente el problema de las *Blue Screen of Death*.

Esta nueva disposición de los anillos permite una mayor flexibilidad en cuanto a la compatibilidad con diferentes dispositivos físicos (*hardware*) ya que estos se ejecutan en dos niveles de privilegio (nivel 1 y 2) dependiendo del controlador en cuanto a que se encuentre certificado por Microsoft o no, garantizando así un mayor rendimiento del equipo.

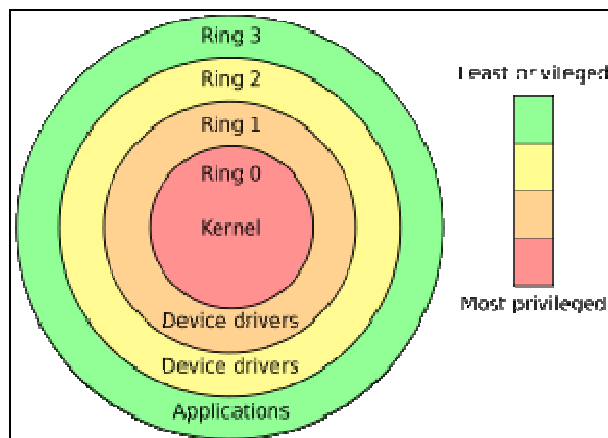


Imagen 2 – Niveles de privilegios en sistemas modernos

En este momento, y cuando se hace evidente la necesidad de implementar las mejoras en el sistema operativo, es necesario mencionar a las actualizaciones ya sea parciales (conocidas como "Patch") o totales, en el caso de un Service Pack o del cambio de versión del sistema operativo.

Las actualizaciones son las que permiten solucionar los problemas que se encuentran en el software que se utiliza diariamente. Cuando un error y/o agujero de seguridad es encontrado en un programa o sistema determinado, se informa al proveedor, el mismo evalúa la importancia del mismo, desarrolla la solución (normalmente llamada "parche") y lanza públicamente la actualización.

En el caso de un Service Pack, generalmente se incluyen paquetes de actualizaciones que solucionan gran cantidad de errores, realizan mejoras, implementan soluciones a nuevos problemas y pueden incluir cambios estructurales en el producto que lo ayudan a soportar de la mejor manera posible los avances tecnológicos. En el caso de que ya no se pueda soportar un producto con estas actualizaciones, el fabricante puede decidir cambiar la versión del producto o incluso lanzar uno nuevo al mercado.

Una de las vías más utilizadas por los atacantes para penetrar sistemas es a través del uso de *exploits* de sistemas que no cuentan con actualizaciones para resolver dichos problemas de seguridad, tanto en forma directa como utilizando "herramientas" como *malware* y otras amenazas informáticas.

Por ello y analizando esta situación, cada fabricante conoce el ciclo de vida de sus productos y, si bien no en todos los casos el cliente debe decidir cambiar, este cambio se comienza a volver necesario con el paso del tiempo y la evolución continua de la tecnología.

Otras mejoras de los sistemas operativos

Un factor de suma importancia en materia de seguridad es el relacionado al sistema de archivos (*File System*) que utilice la plataforma.

Los sistemas operativos antiguos se encuentran basados en el sistema de archivos FAT (File Allocation Table - Tabla de Asignación de Archivos), mientras que los sistemas modernos incorporan, o están basados en, un sistema de archivos más robusto que ofrece mayor seguridad llamado NTFS (New Technology File System – en español, Sistema de Archivos de Nueva Tecnología).

Otra cuestión relacionada con el grado de fortalecimiento de los sistemas operativos modernos respecto de los antiguos radica en la prevención de accesos no autorizados al sistema, lo que comúnmente es explotado por códigos maliciosos, que se propagan a través de determinados puertos del sistema y que, en la mayoría de los casos, cuando han comprometido un equipo intentan enviar al atacante información obtenida en la máquina víctima.

Este inconveniente puede ser mitigado de manera positiva a través de la implementación de un firewall [4] que permite bloquear conexiones salientes. En consecuencia, a partir del SP2 (*Service Pack 2*) de Windows XP, Microsoft activó por defecto el *firewall* personal que en la primera versión del producto se encontraba desactivada.

Por otro lado, un factor sumamente importante en la actualidad es el relacionado con la posibilidad de poder administrar equipos de manera remota, ya sea por razones de mantenimiento de los sistemas, por seguridad o por cuestiones estratégicas en cuanto a la utilización de ciertas tecnologías que requieren determinados protocolos de comunicación.

Para este tipo de tareas se suele utilizar RPC (Remote Procedure Call – en español, Llamada a Procedimiento Remoto), un protocolo que permite establecer una comunicación y ejecutar comandos de manera remota a través de TCP [5] y UDP [6].

RPC es utilizado por determinados programas para acceder a los recursos y servicios de otro equipo de la red de manera remota. En plataformas antiguas no se encuentra disponible en la instalación por defecto, por consiguiente, las aplicaciones que necesitan de este protocolo no funcionan.

En cuestiones de seguridad, son muchas las aplicaciones que deben interactuar con RPC para su correcto funcionamiento. Los programas que admiten administración remota de aplicaciones antivirus es un caso típico, al igual que el uso de aplicaciones de auditoría que permiten revisar, inventariar y mantener esa información actualizada, también de manera remota.

Otro punto importante a destacar es que en sistemas operativos antiguos cualquier perfil de usuario posee privilegios de administración. Esto posibilita, por ejemplo, que códigos maliciosos puedan ejecutar sus instrucciones dañinas sin complicaciones y sin limitaciones en el equipo.

En los SO modernos se pueden crear cuentas de usuarios con privilegios restringidos para establecer determinadas limitaciones en el sistema, como por ejemplo el bloqueo en la instalación de programas o el impedimento de realizar configuraciones en el equipo.

Este tema es un punto muy importante en materia de seguridad, ya que permite prevenir potenciales infecciones de *malware* debido a que, para poder activar sus acciones dañinas, los códigos maliciosos (la mayoría de ellos) necesitan ser ejecutados, es decir, necesitan de la intervención del usuario. Al tener privilegios limitados se previene la ejecución.

Asimismo, la compatibilidad de programas es también un factor sumamente importante que debe ser tenido en cuenta. Muchas aplicaciones necesitan que se cumplan determinadas condiciones netamente relacionadas con nuevas tecnologías y la evolución misma de los SO para funcionar.

Por lo tanto, la mayoría de las aplicaciones actuales se encuentran diseñadas para funcionar en sistemas operativos modernos y no son soportadas por sistemas antiguos. Muchas aplicaciones tampoco son soportadas por plataformas antiguas en su instalación por defecto. Incluso algunos programas de masiva utilización como navegadores web, en sus versiones más recientes, no funcionan en sistemas operativos antiguos. Es el caso de Firefox 3 [7] y el mismo Internet Explorer de Microsoft en su versión 7 [8].

En consecuencia, la utilización de sistemas operativos antiguos debilita la seguridad del sistema y de toda la estructura de red en entornos corporativos, quedando vulnerable a diferentes amenazas que han sido solucionadas en sistemas operativos modernos.

Ventajas de actualizarse

La aparición de tecnologías da lugar al surgimiento de nuevos y potenciales vectores y canales de ataques que dejan de manifiesto la importancia de las actualizaciones de seguridad y, como se ve, existen ventajas que fuerzan a la implementación de sistemas operativos modernos que no se encuentran rezagados únicamente por la falta de apoyo oficial por parte del fabricante, sino que se relacionan con problemas críticos de seguridad.

A lo largo de la evolución que sufrieron las plataformas Windows se fueron mejorando características, que en la actualidad se ven reflejadas en los sistemas modernos, tales como:

- **Mejor compatibilidad con aplicaciones:** en la actualidad, la mayoría de los programas están concebidos para aprovechar toda la potencia que permiten las nuevas tecnologías.
- **Mejor rendimiento de las aplicaciones:** no sólo de los programas sino también del sistema operativo mismo, ya que en los sistemas modernos, las aplicaciones no se ejecutan a nivel del *kernel* (nivel 0) sino que lo hacen a nivel de usuario (nivel 3). El resultado se refleja en la disminución de *BSoD*.
- **Mejor compatibilidad con controladores:** los controladores son programas que permiten utilizar el hardware. En los sistemas operativos antiguos, al ser instalados, también escriben en el nivel 0 (*kernel*). En los sistemas operativos modernos, se ejecutan en el nivel 1 y 2 donde poseen más privilegios que las aplicaciones, pero menores que el *kernel*; en consecuencia, la compatibilidad es mucho mayor y la gestión de recursos más eficiente.
- **Mejor compatibilidad de hardware:** el hardware actual posee funcionalidades que no estaban previstas en los sistemas operativos antiguos y por lo tanto no funcionan. Entre ellos se encuentran el soporte de discos rígidos de mayor tamaño y la tecnología SATA.

- **Mayor seguridad:** Microsoft ha incorporado en los sistemas operativos modernos algunas mejoras en lo que a seguridad se refiere como la característica *PatchGuard*, la Prevención de Ejecución de Datos a través de *hardware* (DEP) y la prevención ante ataques de desbordamiento de búfer (ASLR).



Imagen 3 – Prevención de ejecución de datos (DEP)

Conclusiones

Indudablemente, fortalecer los sistemas podría implicar migrar a determinadas plataformas y/o aplicaciones más seguras, donde, en el caso de los programas, muchos de ellos también requieren de la actualización de la plataforma que los soporta.

Existen suficientes fundamentos que, en materia de seguridad, ponen de manifiesto la importancia de migrar hacia sistemas operativos modernos. Entre los más importantes está el no contar con actualizaciones para sistemas operativos antiguos; en este caso la ventana de vulnerabilidad es considerablemente más amplia, dejando en evidencia los graves problemas que pueden ser aprovechados por personas malintencionadas.

Además, es necesario tener en cuenta que un gran número de códigos maliciosos son distribuidos a través del aprovechamiento de vulnerabilidades y agujeros de seguridad, el no tener la posibilidad de seguir manteniendo al día un sistema operativo, lo hace aún más inseguro.

En consecuencia, en los sistemas operativos actuales de Microsoft, las vulnerabilidades son menores (menores en cantidad, no en grado de criticidad), comparadas siempre con los sistemas antiguos.

Por último, al ser masivamente utilizados, los sistemas operativos de Microsoft suelen ser constantemente atacados intentando explotar diferentes vulnerabilidades que debilitan el sistema; por lo tanto, la instalación de las diferentes actualizaciones de seguridad ayuda notablemente a fortalecerlo.

En este contexto es necesario aclarar que, por supuesto, esta actualización o migración tiene un costo directo asociado que la organización deberá afrontar pero, si se evalúan las alternativas de falta de productividad, el soporte técnico necesario para mantener tecnología obsoleta y, sobre todo, los riesgos de no actualizarse dejando brechas de seguridad y con la posibilidad de sufrir ataques o infecciones, puede verificarse que el costo asociado es igual o mayor.

Más Información:

[1] Internet Explorer

http://es.wikipedia.org/wiki/Internet_Explorer#Internet_Explorer_5

[2] The 25 Worst Tech Products of All Time

http://www.pcworld.com/article/125772-8/the_25_worst_tech_products_of_all_time.html

[3] Protected Mode

<http://msmvps.com/blogs/pmackay/archive/2007/10/15/post22.aspx>

[4] Deteniendo intrusos: firewall personales

<http://eset-la.com/threat-center/1655-deteniendo-intrusos-firewall-personales>

[5] RFC 793 TCP

<http://www.rfc-es.org/rfc/rfc0793-es.txt>

[6] RFC 768 UDP

<http://www.rfc-es.org/rfc/rfc0768-es.txt>

[7] Requerimientos de Firefox 3

<http://www.mozilla-europe.org/es/firefox/system-requirements/>

[8] Requerimientos de Internet Explorer 7

<http://www.microsoft.com/spain/windows/downloads/ie/sysreq.mspx>

[9] Fin del soporte técnico para Windows 98 y Windows Me

<http://www.microsoft.com/latam/windows/soporte/endofsupport.mspx>

[10] Computación confiable

<http://www.microsoft.com/latam/twc2/default.mspx>

Anexo: Antecedentes históricos y datos interesantes

El primer sistema operativo (SO) comercializado por Microsoft fue liberado en 1981 y constituyó la primera versión de MS-DOS (Microsoft Disk Operating System, en español Sistema Operativo de Disco de Microsoft); un sistema operativo operado bajo línea de comandos. Dos años más tarde, salía una nueva versión, MS-DOS 2.0, que incorporaba un intérprete de comandos (*shell*); en 1984 salió MS-DOS 3.0 y continuaron publicándose nuevas versiones hasta alcanzar la 6.22 de MS-DOS en 1994.

Luego, con el ánimo de incorporar una Interfaz Gráfica de Usuario (GUI), Microsoft creó su primer entorno gráfico bajo el nombre Windows, comenzando de esta manera la notable evolución de sus sistemas operativos.

La primera versión de este entorno gráfico, liberada en 1985, se llamó Windows 1.0. Posteriormente aparecerían las versiones 2.0 en 1987 y 3.0 en 1990. Durante 1992 se lanzó Windows 3.1 que podía ser utilizado sólo por un usuario en un determinado tiempo (monousuario) y ejecutar una sola tarea en el mismo momento (monotarea). En octubre de ese año se lanzó Windows 3.11 con funcionalidades orientadas a redes corporativas.

Con la intención de desarrollar un sistema operativo más robusto, competitivo y orientado a entornos corporativos, en 1993 Microsoft lanzó al mercado Microsoft Windows NT (New Technology – Nueva Tecnología) marcando un salto importante respecto a los sistemas utilizados hasta ese entonces. Windows NT, a diferencia de sus antecesores, era un sistema operativo multiusuario y multitarea en el cual se basarían los sucesivos SO.

Con la intención de sustituir a MS-DOS como SO y a Windows 3.11 como entorno gráfico, el 24 de agosto de 1995 Microsoft lanzaba de manera oficial Microsoft Windows 95, dando origen a una nueva generación de sistemas operativos.

Windows 95 fue sustituido por Microsoft Windows 98 el 25 de junio de 1998. Casi un año más tarde, durante mayo de 1999, se lanzaba una actualización para este SO denominado Microsoft Windows 98 SE (Second Edition – Segunda Edición) que incorporaba el navegador web Internet Explorer 5 [1] como parte del sistema.

En el 2000 un nuevo sistema operativo fue puesto a disposición de los usuarios, y significó un cambio en la nomenclatura de los sistemas basados en tecnología NT. En febrero de ese mismo año se lanzó este producto bajo el nombre de Microsoft Windows 2000, también conocido como Win2K y diseñado para ambientes corporativos.

Paralelamente, en septiembre del 2000, la empresa incorporaba al mercado Microsoft Windows ME (Millennium Edition – Edición Milenio), un SO orientado a entornos hogareños que, según un artículo publicado por la revista PC World, fue considerado uno de los “peores productos de todos los tiempos” [2].

Poco tiempo después, durante el año 2001, se daba inicio a una “nueva generación” de sistemas operativos con el lanzamiento de Microsoft Windows XP (eXPerience - Experiencia), un producto basado en el código de Windows 2000 y un renovado entorno gráfico.

En enero de 2007, Microsoft comercializaba a nivel mundial su versión de sistema operativo más reciente hasta el momento: Microsoft Windows Vista, cuya interfaz gráfica fue completamente rediseñada.

Otro dato particular es que durante julio del 2006, Microsoft presentó una versión de Windows XP orientada a soportar hardware antiguo denominado Microsoft Windows Fundamentals for Legacy PCs - Windows Fundamental para computadoras antiguas.

Glosario

Amenaza: agente capaz de aprovechar fallos de seguridad o debilidades de un sistema informático.

ASLR: acrónimo de *Address Space Layout Randomization*. Funcionalidad implementada por Microsoft en Windows Vista destinada a prevenir ataques de desbordamiento de búfer (*Buffer Overflow*).

Ataque: acción de vulnerar esquemas de seguridad explotando algún tipo de debilidad del sistema o problema a nivel de *software* o *hardware* en el equipo.

BSoD: acrónimo de *Blue Screen of Death* (Pantalla Azul de la Muerte). Pantalla que muestra un sistema operativo Windows cuando se produce un error en el *kernel* del mismo.

DEP: acrónimo de *Data Execution Prevention*. Característica de seguridad incorporada por Microsoft en los sistemas operativos modernos a partir de Windows XP SP2 diseñado para prevenir la ejecución de programas y servicios en determinadas regiones de la memoria.

FAT: acrónimo de *File Allocation Table* (Tabla de Asignación de Archivos). Sistema de archivos utilizado por las versiones antiguas de MS Windows.

Firewall: sistema que se coloca entre un sistema (generalmente una red local LAN) e Internet permitiendo asegurar las comunicaciones entre dicha red e Internet a través de reglas de filtrado.

GUI: acrónimo de *Graphical User Interface* (Interfaz Gráfica de Usuario). Entorno constituido por un conjunto de imágenes gráficas que permiten representar la información en pantalla de una manera amigable.

Hardware: conjunto de elementos físicos que componen una computadora.

LAN: acrónimo de *Local Area Network* (Red de Área Local). Permite interconectar equipos entre sí con la finalidad de compartir recursos.

Legacy System: sistemas operativos o aplicaciones antiguas.

Malware: programa o porción de código que provoca algún tipo de anomalía en un sistema informático.

NTFS: acrónimo de *New Technology File System* (Sistema de Archivos de Nueva Tecnología). Sistema de archivos utilizado por las versiones modernas de sistemas operativos de Microsoft.

PatchGuard: *Kernel Patch Protection* (Protección contra revisiones del núcleo). Tecnología incorporada por Microsoft a los sistemas operativos de 64-bits tendiente a prevenir el parche del *kernel*.

SATA: acrónimo de *Serial Advanced Technology Attachment*. Tecnología que permite la transmisión de datos entre el *Motherboard* (Placa madre) y determinados dispositivos de almacenamiento como el disco rígido.

Shell: entorno que permite e interpreta la ejecución de comandos en un sistema operativo. También se lo conoce como CLI (*Command Line Interface* – Intérprete de Línea de Comandos).

Sistema Operativo Monousuario: se refiere a la característica de determinados sistemas operativos en los que sólo pueden ser ocupados por un único usuario en un determinado momento.

Sistema Operativo Multiusuario: característica de determinados sistemas operativos que posibilita la ejecución de tareas por múltiples usuarios en un determinado momento.

SO: acrónimo de Sistema Operativo. Conjunto de programas que permite administrar los recursos del sistema.

Software: conjunto de programas que pueden ser ejecutados por el hardware para realizar tareas solicitadas bajo demanda de los usuarios

TCP: acrónimo de *Transmission Control Protocol* (Protocolo de Control de Transmisión). Protocolo de comunicación que trabaja en capa 3 (capa de transporte) del modelo TCP/IP y en capa 4 (capa de transporte) del modelo de referencia OSI. Es utilizado por el protocolo IP para el envío de datos.

Vulnerabilidad: debilidad en un sistema de información que puede ser potencialmente aprovechada por una amenaza.

Security updates: corrigen un determinado error o vulnerabilidad de seguridad.

UDP: acrónimo de *User Datagram Protocol* (Protocolo de Datagramas de Usuario). Protocolo que trabaja en capa 3 del modelo TCP/IP (Capa de transporte) y capa 4 del modelo de referencia OSI (capa de transporte). UDP puede enviar datagramas (paquetes de datos) en una red sin la necesidad de establecer conexión.

Update rollups: conjunto de parches de seguridad.

Service packs: conjunto de actualizaciones que corrigen y/o agregan mejoras a productos de Microsoft.