Eleven Paths

Informe sobre_

SmartScreen

Telefónica CYBER SECURITY UNIT

elevenpaths.com

Contenido

¿Qué es SmartScreen? 2
Análisis de Funcionamiento 5
Posibles Evasiones 8
Contramedidas y conclusiones 12

¿Qué es SmartScreen?

SmartScreen es un componente de Windows Defender orientado a proteger a los usuarios contra ataques potencialmente dañinos, ya sea en forma de enlaces o ficheros. Está incluido con este nombre desde el Internet Explorer 8 en Windows 7, y añadió la protección contra ejecutables en Internet Explorer 9. En Windows 8 se introdujo esta protección de reputación de binarios en todo el sistema operativo.

Cuando un usuario se encuentra navegando por Internet, el filtro o componente SmartScreen analiza los sitios que está visitando y, en caso de ingresar a uno considerado sospechoso, muestra un mensaje de advertencia para que el usuario decida si desea continuar o no. Para realizar esta actividad, utiliza una lista dinámica de los sitios de phishing y de los dominios que utilizan los códigos maliciosos y, si son sitios ya reportados, bloquea el acceso.

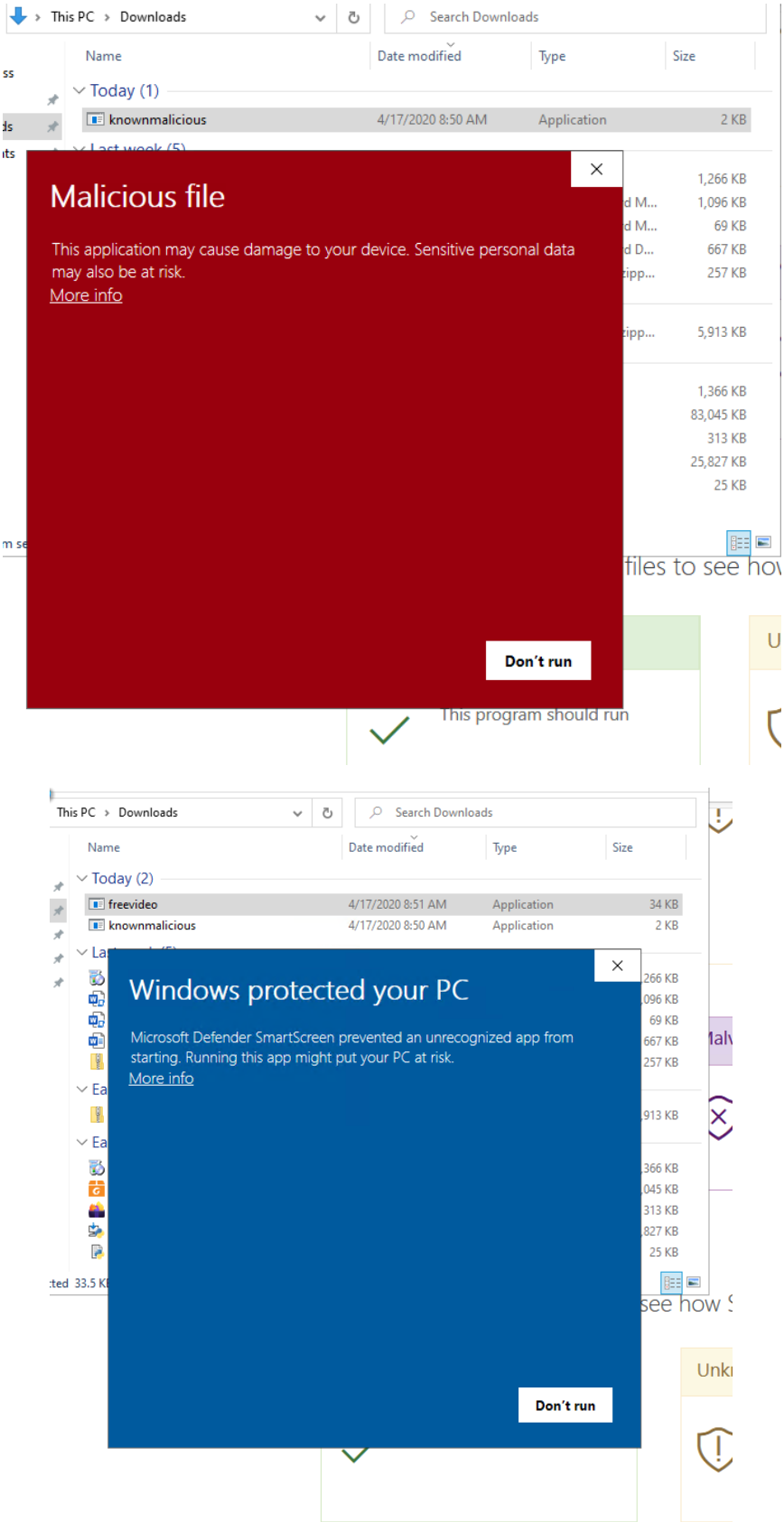
En el caso de los archivos descargados, SmartScreen realiza una verificación sobre ellos verificando su reputación en base a la información recolectada de otros usuarios de los productos de Microsoft.

En resumen, según la web de su propio creador[1], Microsoft, SmartScreen ofrece las siguientes ventajas:

- Anti-Phishing y Anti-Malware.
- Protección de aplicaciones basado en la reputación de las URL.
- Integrado con el Sistema Operativo.
- Heurística y Diagnóstico de Datos mejorados.
- Administración y configuración a través de GPO y Microsoft Intune.
- Bloqueo de URLs asociado a aplicaciones no deseadas.

El objetivo de SmartScreen es bastante claro y ha sido analizado en varios sitios. Sin embargo, para este informe nos centramos en tratar de entender cómo funciona SmartScreen particularmente en los archivos descargados en el sistema. **Hemos intentado comprender cuáles son los disparadores que activan este componente de protección desarrollado por Microsoft para conocer mejor su eficacia.**

[1] Windows Defender SmartScreen. [En línea]. Available: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-smartscreen/windows-defender-smartscreen-overview.



¿Qué es Alternate Data Stream?

Para entender cómo actúa SmartScreen sobre los archivos descargados, primero debemos introducir los ADS. Alternate Data Streams o ADS es una característica propia del sistema de archivos NTFS desarrollado por Microsoft e incluida desde la época de Windows NT (año 1993). ADS permite almacenar metadatos en un archivo, ya sea por medio de un stream directamente o de otro archivo o fichero. La forma más común de uso por medio de la línea de comandos es escribiendo:

```
echo texto escondido >archivoOriginal.txt:archivoAEsconder.txt
```

y para visualizarlo, en vez de ejecutar un *type archivoOriginal.txt*, ya que así verían la información *archivoOriginal.txt*, ejecutaban:

```
type archivoOriginal.txt:archivoAEsconder.txt
texto escondido
```

En los 90, muchos usaban ADS para esconder información dentro de un archivo por la escasa documentación que existía en su momento. También algunos software escondían código malicioso utilizando estas técnicas. Sin embargo, no solo fue utilizado con fines maliciosos, sino todo lo contrario. Algunos otros productos lo han utilizado para para diferentes acciones, como es el caso del antivirus Kaspersky, que lo utilizaba para guardar los resultados de los archivos escaneados en el mismo archivo como un ADS.

Actualmente los ADS también son utilizados por diferentes productos para marcar archivos en el stream *":Zone.Identifier"* para saber cuándo un archivo es externo (es decir, que no fue creado en el propio equipo) y debe por tanto ser examinado por SmartScreen. Dada esta característica, Microsoft comenzó a marcar todos los archivos descargados a través de Internet Explorer (en su momento), otros desarrolladores de navegadores comenzaron a hacer lo mismo para aprovechar la protección de SmartScreen.

El valor que se escribe en el Stream, es decir el ZoneId, puede tener cualquier valor que uno desee. Sin embargo, el comportamiento de SmartScreen se rige de los valores reflejados en la Tabla 1:

Identifier	Value
URLZONE_LOCAL_MACHINE	0
URLZONE_INTRANET	1
URLZONE_TRUSTED	2
URLZONE_INTERNET	3
URLZONE_UNTRUSTED	4

Tabla 1. Fuente: https://docs.microsoft.com/en-us/dotnet/api/microsoft.visualstudio.ole.interop.urlzone.

Lo más interesante a destacar de la tabla, es que el componente SmartScreen sólo actuará si el valor del ZoneId = 3.

Se sabe que los programas que toman en cuenta el ZoneId con objetivo de transmitir información sobre el origen de los archivos son Microsoft Edge, Internet Explorer y Outlook, pero ¿lo aprovechan otros programas populares que sí descargan ficheros desde Internet?

Análisis de Funcionamiento

Hemos decidido plantear una serie de preguntas y analizar cada caso para entender mejor la eficacia de la protección que nos brinda el propio sistema operativo ante posibles archivos maliciosos descargados en nuestro equipo. La primera pregunta, y quizás la más obvia, partiendo de que la solución fue pensada para protegernos cuando descargamos un archivo con el navegador nativo, es:

¿Qué otro navegador debería tener ese comportamiento? Es decir, ¿cuáles marcan con ZoneID = 3 el archivo descargado?

Analizamos los 10 navegadores más usados en sistemas operativos de escritorio, según la publicación de NetMarketShare[2]. Para ello, instalamos la última versión de cada uno a enero de 2020 y con ellos descargamos un archivo de una página web. **¿Se agrega el ZoneId al archivo descargado?**

Como puede verse en la siguiente Tabla 2, la gran mayoría sí marcan los archivos descargados con ZoneID = 3. Aunque se observa que en Internet Explorer (ya sin soporte), la implementación original solo contemplaba la marcación de archivos ejecutables y no del resto de los archivos. El único navegador de los más usados actualmente en el mercado que hace caso omiso por completo de esta característica es Baidu. Solo el 10 % no implementa el ZoneID = 3 para los archivos descargados, requerido para que SmartScreen los analice.

Navegador	ZoneId agregado
Chrome	Sí
Firefox	Sí
Internet Explorer	Solo para archivos ejecutables
Edge	Sí
Sogou Explorer	Sí
Opera	Sí
QQ	Sí
Yandex	Sí
UC Browser	Sí
Baidu	No

Tabla 2. Uso de ZoneId por los navegadores más populares del mercado.

¿Y qué sucede con los clientes de mail?

Para responder a esta pregunta, buscamos en foros y portales cuáles eran los clientes de correo más populares durante el 2019, al no existir una lista oficial equivalente de los más usados a los navegadores. Enviamos un documento por correo y determinamos si al guardar el adjunto en el disco, éste quedaba marcado con el ZoneID = 3.

[2] https://netmarketshare.com/

El resultado aparece reflejado en la Tabla 3. Menos del 50% de los clientes de correo han marcado los archivos con el ZoneId = 3.

Cliente de correo	ZoneId agregado
Outlook	Sí
Windows Live Mail	Sí
Thunderbird	Sí
eM Client	No
Mailbird	No
Mailspring	No
Sylpheed	No

Tabla 3. Uso de ZoneId por los clientes de correo más populares del mercado.

Parece que esta protección es menos implementada en los clientes de correo que en los navegadores. Dado que apenas tiene contraindicaciones su uso, ¿es posible que os desarrolladores de software quizás no conozcan esta característica? Con esto en mente, la pregunta siguiente fue un poco más amplia: **¿Qué otro tipo de software podría utilizar habitualmente un usuario para descargar archivos de Internet?**

Es así como decidimos analizar el tipo de software más común que un usuario actual tendría instalado en sus equipos y que les permitiría descargar software que podría ser malicioso, pero que SmartScreen ni siquiera analizaría por no tener el ZoneID = 3. El tipo de software que decidimos analizar ha sido:

- Clientes de Mensajería Instantánea
- Clientes de FTP
- Software de Versionado de Código
- Sincronizadores de Cloud

Clientes de Mensajería Instantánea

De los clientes de mensajería instantánea, el 42 % no implementa el ZoneID = 3 para los archivos descargados, requerido para que SmartScreen los analice.

Cliente de mensajería instantánea	ZoneId agregado
Telegram Desktop	No
Pidgin	No
Signal	Sí
Riot	Usa Internet Explorer
Slack	Sí
Wire	Sí
Discord	Usa browser default
Viber	No
WhatsApp	Sí
Line	No
Skype	No
Microsoft Teams	Sí

Tabla 4. Uso de ZoneId por los clientes de mensajería instantánea más populares del mercado.

Clientes de FTP

De los clientes de FTP analizados, el 86 % no implementa el ZoneID = 3 para los archivos descargados, requerido para que SmartScreen los analice.

Cliente de FTP	ZoneId agregado
FileZilla	No
WinSCP	No
Cyberduck	No
Coffee Cup Direct FTP	No
Solar Putty	No
MonstaFTP	Usa el navegador

Tabla 5. Uso de ZoneId por los clientes de FTP más populares del mercado.

Clientes de versionado de Código

De los versionadores de Código analizados, el 100 % no implementa el ZoneID = 3 para los archivos transferidos, requerido para que SmartScreen los analice.

Cliente de Versionado de Código	ZoneId agregado
Github Client	No
Git-scm	No
TortoiseHG	No
TortoiseSVN	No

Tabla 6. Uso de ZoneId por los clientes de versionado de código más populares del mercado.

Clientes de Sincronización en la Nube

De los clientes de Sincronización en la Nube analizados, el 100 % no implementa el ZoneID = 3 para los archivos descargados, requerido para que SmartScreen los analice.

Cliente de Sincronización en la Nube	ZoneId agregado
Insync	No
Dropbox	No
Google Sync	No
OneDrive	No
GoodSync	No
Odrive	No

Tabla 7. Uso de ZoneId por los clientes de sincronización en la nube más populares del mercado.

Transferencias de archivos

Pero también decidimos probar qué sucede con las transferencias de archivos más tradicionales, es decir qué sucede cuando copiamos un archivo a través de un recurso compartido de red, transferencia a través de bluetooth o al utilizar PowerShell WebClient, con las propias utilidades de Microsoft, y el resultado fue el siguiente:

Mecanismo de transferencia de archivos	ZoneId agregado
Microsoft Bluetooth	No
Carpeta compartida	No
Powershell WebClient	No

Tabla 8. Uso de ZoneId por otros mecanismos de transferencia de archivos.

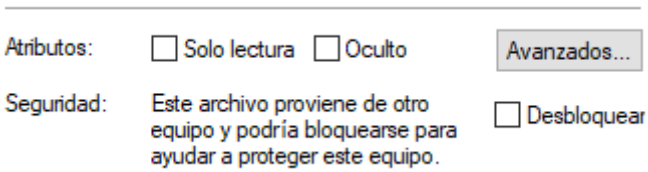
Posibles Evasiones

Tras entender cómo y cuándo se marca el archivo, la investigación nos llevó a reflexionar sobre **qué proceso se encarga de ejecutar SmartScreen y si existen formas de eludir esa ejecución bajo su supervisión**. Para realizar la prueba, marcamos archivos en su mayoría interpretados y conocidos como maliciosos por SmartScreen para saber si el archivo ejecutado de esta forma eludía o no la supervisión de SmartScreen. Tomamos una serie de ficheros en diferentes lenguajes interpretados y les activamos el bit.

Es simple:

```
echo [ZoneTransfer] > knownmalicious.py:Zone.Identifier
echo ZoneId=3 >> knownmalicious.py:Zone.Identifier
```

Para saber si se ha activado, en las propiedades del archivo aparecerá el siguiente mensaje:



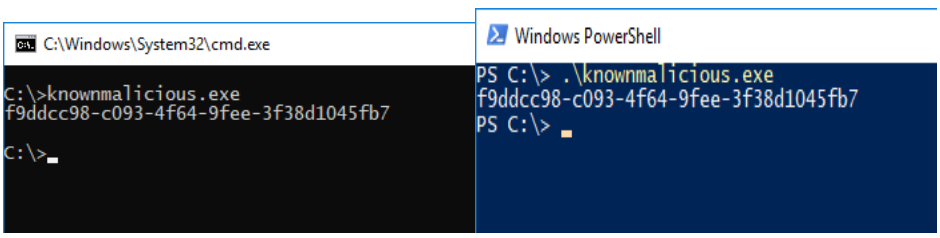
Si se elimina el atributo o se marca la opción "Desbloquear", desaparecerá esa advertencia de seguridad de sus propiedades.

Los resultados aparecen en esta tabla:

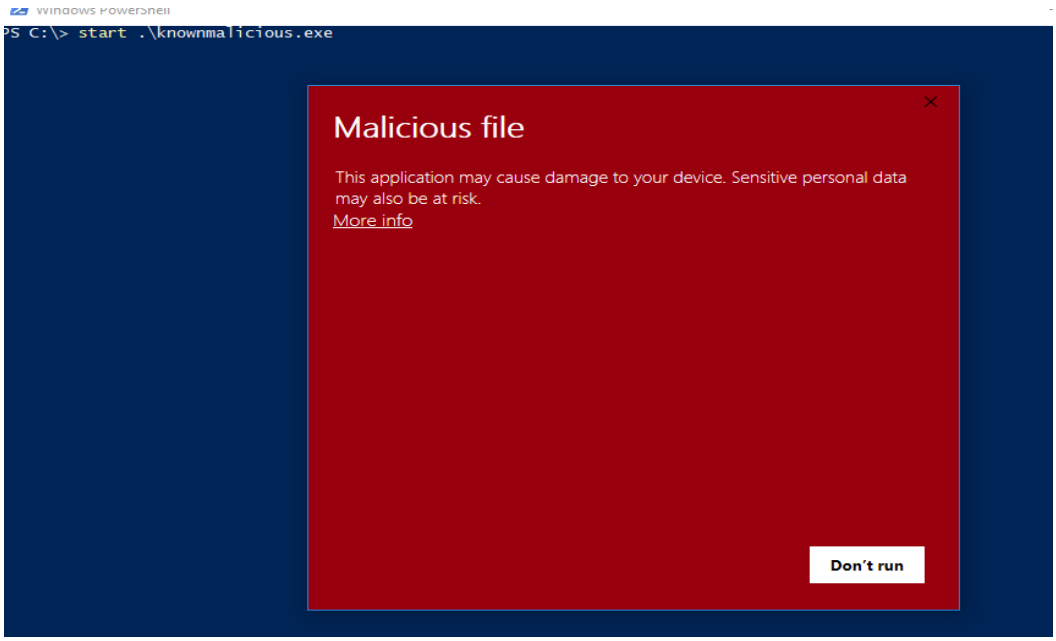
Acción	Resultado	Nota
Doble clic .exe malicioso	No elude SmartScreen	
Doble clic .vbs malicioso	No actúa SmartScreen	Aparece una alerta (ver ilustración más abajo)
Doble clic .vbe malicioso	No elude SmartScreen	
Doble clic .bat malicioso	No elude SmartScreen	
Doble clic .msi malicioso	No elude SmartScreen	
Doble clic .com malicioso	No elude SmartScreen	
Doble clic .cpl malicioso	No elude SmartScreen	
Doble clic .jse malicioso	No elude SmartScreen	
Doble clic .scr malicioso	No elude SmartScreen	
Doble clic .wsf	No actúa SmartScreen	Aparece una alerta
Doble clic .py	No actúa SmartScreen	
Lanzados con "start" desde consola cmd	No actúa SmartScreen	
Lanzados con "start" desde consola powershell	No elude SmartScreen.	
Ejecución directa en cmd	No actúa SmartScreen	
Ejecución directa en powershell	No actúa SmartScreen	
Doble clic en Carpeta Compartida	No actúa SmartScreen	Aparece una alerta
Ejecución desde menú contextual	No actúa SmartScreen	
Ejecución desde Task Scheduler	No actúa SmartScreen	

Tabla 9.

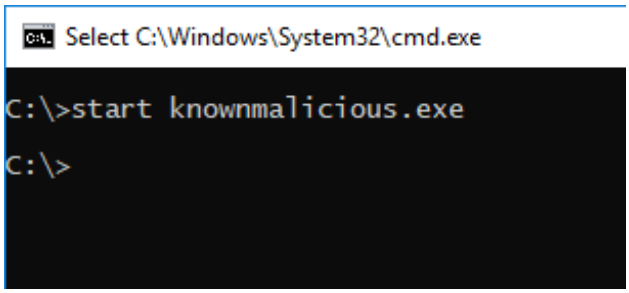
Algunos ejemplos de cómo hemos lanzado los ejecutables (la impresión del código indica que el malware que debería haber detenido SmartScreen se ha ejecutado con éxito):



Quizás lo más curioso es la diferencia al lanzarlos con el comando "start":

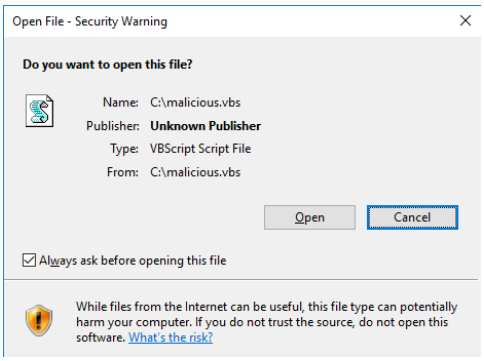


En el que SmartScreen se interpone en PowerShell, pero no en CMD.



Por cierto, el hecho de marcar el ejecutable que realiza la interpretación de los programas (python.exe, cmd.exe, cscript.exe, powershell.exe) no influye. La tabla quedaría igual.

En ciertos casos aparece la siguiente alerta:



Por último, comprobamos un tipo de software que se utiliza habitualmente para transferir un archivo de un lugar a otro: los compresores de ficheros. ¿Respetan esta marca? Es decir, quisimos comprobar si la marca se mantiene tras la

descarga, compresión y descompresión. ¿Se mantiene el ZoneID=3 para que pase que siga siendo analizado por SmartScreen tras la descarga? Las conclusiones aparecen en la Tabla 10. De los compresores y descompresores de archivos analizados, el 75 % no implementa el ZoneID = 3 requerido para que SmartScreen los analice en archivos una vez que son descomprimidos.

Descompresor	ZoneId conservado
7zip	No
Descompresor Windows	Sí
PeaZip	No
Ashampoo Zip	No
Zipware	No
Hamster Zip Archiver	No
Winrar	No
Winzip	Sí

Tabla 10. ZoneId conservador tras la operación de algunos compresores/descompresores.

Contramedidas y conclusiones

Durante este informe nos hemos centrado en dos enfoques diferentes. Los desarrolladores de software que respetan o no la marca que permite que Windows analice los ficheros con SmartScreen y el software que, con el archivo marcado, invoca a no a esta protección.

Para el primero de los enfoques no hay en principio una contramedida concreta más que los programadores utilicen en mayor medida esta característica. La solución parece pasar por una mayor difusión y concienciación del problema para que comiencen a implementarlo. Es importante que los programas encargados de descargar en general archivos sean conscientes de la tabla de orígenes de ficheros, en concreto del ZoneId. Esto les permite colaborar con SmartScreen para mejorar la seguridad de los usuarios.

En la Imagen se encuentra un extracto de código implementado por Mozilla Firefox donde se inserta el ZoneId a un archivo descargado. No es algo que requiera demasiado esfuerzo de implementar. Para el segundo de los escenarios, el programa que ejecuta código interpretado podría ser en mayor medida el encargado de llamar a SmartScreen si encuentra la marca.

```
try {
  let zoneId = "[ZoneTransfer]\r\nZoneId=" + zone + "\r\n";
  let { url, isPrivate, referrerInfo } = aDownload.source;
  if (!isPrivate) {
    let referrer = referrerInfo
      ? referrerInfo.computedReferrerSpec
      : "";
    zoneId +=
      this._zoneIdKey("ReferrerUrl", referrer) +
      this._zoneIdKey("HostUrl", url, "about:internet");
  }
  await stream.write(new TextEncoder().encode(zoneId));
} finally {
  await stream.close();
}
```

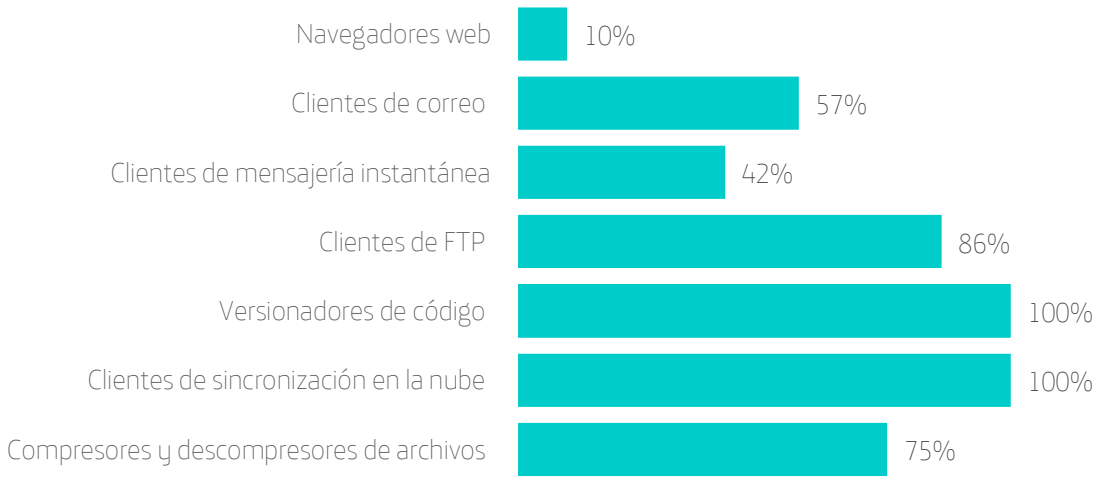
En general, de acuerdo con el análisis realizado se desprenden las siguientes conclusiones:

- En el caso de los **navegadores web, solo el 10 % no implementa el ZoneID = 3** para los archivos descargados, requerido para que SmartScreen los analice.
- De los **clientes de correo analizados, el 57 % no implementa el ZoneID = 3** para los archivos adjuntos, requerido para que SmartScreen los analice.
- De los **clientes de mensajería instantánea, el 42 % no implementa el ZoneID = 3** para los archivos descargados, requerido para que SmartScreen los analice.
- De los **clientes de FTP analizados, el 86 % no implementa el ZoneID = 3** para los archivos descargados, requerido para que SmartScreen los analice.
- De los **versionadores de Código analizados, el 100 % no implementa el ZoneID = 3** para los archivos transferidos, requerido para que SmartScreen los analice

- De los **clientes de Sincronización en la Nube analizados, el 100 % no implementa el ZoneID = 3** para los archivos descargados, requerido para que SmartScreen los analice
- De los **compresores y descompresores de archivos analizados, el 75 % no implementa el ZoneID = 3** requerido para que SmartScreen los analice en archivos una vez que son descomprimidos.

LOS NAVEGADORES WEB SON LOS QUE MEJOR IMPLANTAN SMARTSCREEN

Porcentaje de tecnologías analizadas que no implantan el ZoneID = 3 para los archivos descargados



De esta manera, podemos concluir que un potencial atacante tendría varias formas de hacer llegar un archivo malicioso a un equipo con mayores garantías de no ser descubierto por **SmartScreen:** confiando en que el usuario descargue ejecutables con ciertos programas u obligándolo a hacerlo a través de programas que no lo implementan en absoluto.

Resulta necesario que los desarrolladores estén concienciados sobre cómo funciona **SmartScreen** para aprovechar sus capacidades de detección y proteger mejor al usuario.

Acerca de ElevenPaths

En ElevenPaths, la unidad global de ciberseguridad del Grupo Telefónica, creemos que es posible un mundo digital más seguro. Apoyamos a nuestros clientes en su **transformación digital,** creando **innovación disruptiva**, aportando la privacidad y la confianza necesaria en nuestra vida digital diaria.

Combinamos la frescura y energía de una start-up con la potencia, conocimiento y robustez de Telefónica, contribuyendo con soluciones que posibilitan la prevención, detección y respuesta ante amenazas diarias en nuestro mundo digital.

Generamos alianzas estratégicas que permiten ampliar la seguridad de nuestros clientes y, además, colaboramos con organismos y entidades como la Comisión Europea, CyberThreat Alliance, ECSO, EuroPol, Incibe, y la Organización de los Estados Americanos (OEA).