Uno de los métodos más comunes de propagar malware es por medio de los archivos adjuntos en correos electrónicos, que se ejecutan al tratar de abrir el archivo adjunto, aún cuando proviene de remitentes supuestamente confiables.

Debido a esto, Microsoft planea incluir en la lista negra 38 extensiones de archivo adicionales para que no se puedan descargar como archivos adjuntos en Outlook web.

Anteriormente conocido como aplicación web de Outlook u OWA, el cliente de correo electrónico basado en la web de Microsoft para que los usuarios accedan a correos electrónicos, calendarios, tareas y contactos desde el servidor Exchange local de Microsoft y Exchange Online basado en la nube.

Entre las 104 extensiones de archivos bloqueadas se incluyen .exe, .url, .com, .cmd, .asp, .lnk, .js, .jar, .tmp, .app, .isp, .hlp, .pif, .msi, .msh, entre otras.

Ahora, la lista de bloqueo ampliada también incluirá 38 nuevas extensiones en una nueva actualización, evitando que los usuarios de Outlook en la web descarguen archivos adjuntos que tengan cualquiera de las 142 extensiones de archivo, hasta que un administrador de Outlook o Microsoft Exchange Server haya incluido en la lista blanca alguna de las extensiones eliminándola de la lista BlockedFileTypes.

> *«Siempre estamos evaluando formas de mejorar la seguridad para nuestros clientes, por lo que nos tomamos el tiempo de auditar la lista de archivos bloqueados existentes y actualizarla para reflejar mejor los tipos de archivos que vemos como riesgos hoy. Los tipos de archivos recientemente bloqueados rara vez se utilizan, por lo que la mayoría de las organizaciones no se verán afectadas por el cambio. Sin embargo, si sus usuarios envían y reciben archivos adjuntos afectados, informarán que ya no pueden descargarlos»*, dijo Microsoft en su blog.

Algunas de las extensiones de archivos recientemente añadidas a la lista negra son:

- Extensiones de archivos utilizadas por el lenguaje Python: .py, .pyc, .pyo, .pyw, .pyz, .pyzw
- Extensiones utilizadas por el lenguaje de PowerShell: .ps1, .ps1xml, .ps2, .ps2xml, .psc1, .psc2, .psd1, ,psdm1, .psd1, .psdm1
- Extensiones utilizadas por certificados digitales: .cer, .crt, .der
- Extensiones utilizadas por el lenguaje Java: .jar, .jnlp
- Extensiones utilizadas por distintas aplicaciones: .appcontent-ms, .settingcontent-ms, .cnt, .hpj, .website, .webpnp, .mcf, .prrinterexport, .pl, .theme, .vbp, .xbap, .xll, .xnk, .msu, .diagcab, .grp

Microsoft escribió que si bien las vulnerabilidades asociadas con varias aplicaciones han sido parcheadas, *«están siendo bloqueadas en beneficio de organizaciones que aún podrían tener versiones anteriores del software de la aplicación en uso».*

> *«La seguridad de los datos de nuestros clientes es nuestra máxima prioridad, y esperamos que nuestros clientes comprendan y aprecien este cambio. El cambio puede ser perjudicial, por lo que esperamos que la información aquí explique lo que estamos haciendo y por qué»*, dijo Microsoft

Por otro lado, Google, el proveedor de correo electrónico Gmail, también mantiene una lista de extensiones de archivos bloqueados que la compañía considera perjudiciales para sus usuarios de Gmail.