Phishing a través de Microsoft Teams que descarga malware

Recursos Afectados

Cualquier empresario, autónomo o empleado que haga uso de Microsoft Teams en su entorno laboral.

Descripción

Se ha detectado un ciberataque de tipo phishing a numerosos trabajadores de una misma empresa. Los empleados recibieron a través del servicio corporativo de Microsoft Teams un mensaje fraudulento que invitaba a descargar un archivo .zip con códigos maliciosos, que en caso de ser descargados y ejecutados, podrían generar efectos considerablemente negativos. Microsoft, desarrollador de Teams, ha reportado indicios de una nueva modalidad de phishing basada en equipos que afectó a otras empresas en julio de este mismo año. Diversos elementos de este nuevo phishing coinciden con el modus operandi descrito por Microsoft.

Solución

En caso de recibir una comunicación de Teams como las que se describen en este aviso, es recomendable ignorarlo, eliminarlo e inmediatamente ponerlo en conocimiento del resto de empleados para evitar posibles nuevas víctimas. Además, se recomiendan las siguientes medidas adicionales:

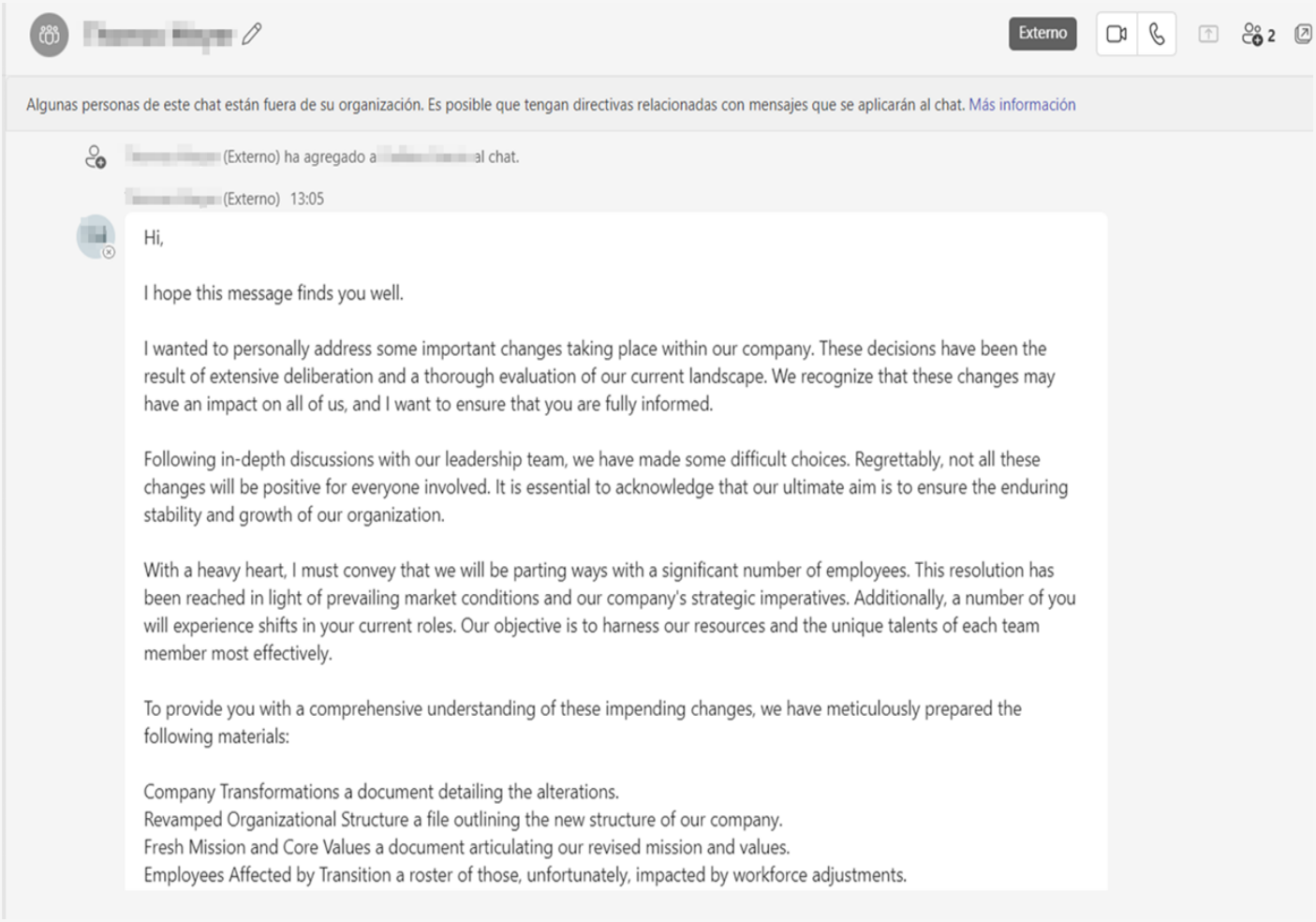
- Endurecer la política federativa de Teams. En lugar de emplear una política negativa que bloquee dominios, será más eficiente establecer una política positiva que bloquee, es decir, aceptar solo dominios confiables.
- Si en los logs (historiales de actividad) se detecta el intento de conexión a alguna dirección IP desconocida o sospechosa, se recomienda crear reglas para bloquear el acceso a estas, como medida preventiva.
- Reportar el tenant o inquilino malicioso a Microsoft, es decir, denunciar el usuario o cuenta desde la que proceden los mensajes.
- Denunciar a las autoridades pertinentes, tales como Policía Nacional o Unidad de Delitos Telemáticos de la Guardia Civil, y poner en conocimiento de INCIBE el caso.

El phishing es uno de los fraudes más replicados en empresas de todos los sectores. Para combatirlo es crucial saber reconocerlo. Descubre en esta historia real el caso de un empleado que no prestó la suficiente atención y cayó en la trampa.

Detalle

El mensaje reportado por la empresa que ha sido atacada cuenta con elementos en común con los reportados por Microsoft en su informe de nuevas vulnerabilidades.

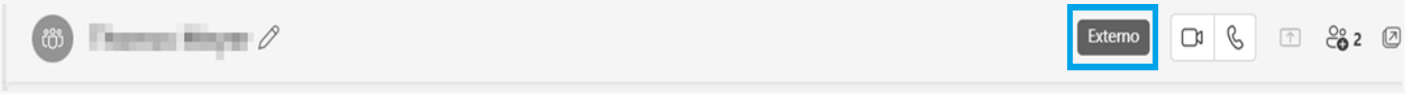
En este caso, un total de 107 trabajadores recibieron a través de su servicio corporativo de Microsoft Teams un mensaje en inglés, informando de cambios organizativos muy significativos en la empresa con un archivo .zip adjunto con supuesta información adicional.



Para hacer llegar el mensaje a los trabajadores, el atacante empleó una dirección de Office365 con la que inició sesión en Microsoft Teams y creó un grupo, abusando de las políticas de federación, con las más de 100 direcciones de correo de los empleados afectados.

Para hacerlo más creíble suplantó la identidad del presidente de la empresa en cuestión, firmando con su nombre, y dotó al mensaje de importancia y urgencia, elementos propios del phishing. Así pues, ya encontramos los dos primeros elementos que hacen sospechar del mensaje. En primer lugar, que el interlocutor es el presidente de la empresa, algo muy poco común, y segundo, que el cuerpo del mensaje denota urgencia y exige una respuesta rápida, algo que se replica constantemente en el phishing.

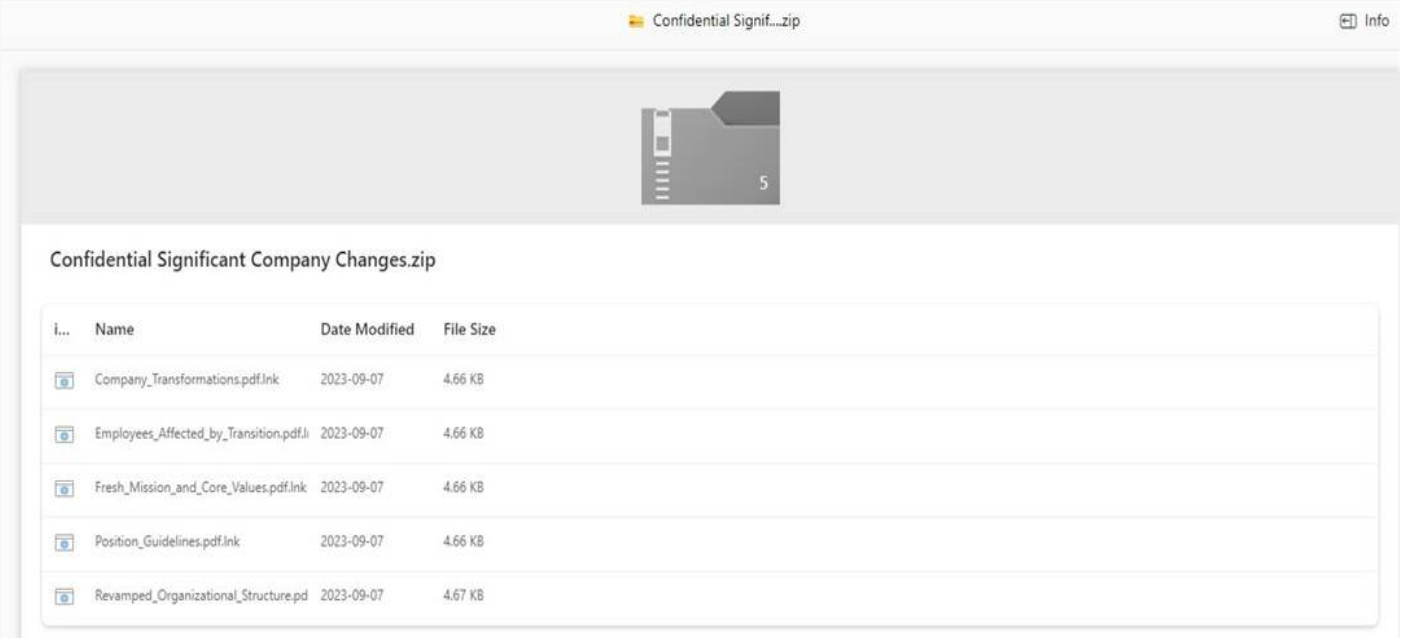
El tercer elemento que hace sospechar del mensaje tiene que ver con la etiqueta “Externo” que aparece junto al usuario.



Esto revela que el usuario que ha creado el grupo y difundido los mensajes pertenece a unos círculos externos a los de la empresa. Por tanto, se cuenta con un elemento de peso para desconfiar de la autenticidad del mensaje.

Incluido en el mensaje se adjunta un fichero tipo .zip que aparentemente recopila los cambios en la compañía de los que se habla en el mensaje.

Dicho fichero contiene archivos maliciosos que podrían tener graves consecuencias en el equipo en que se descarguen. Si se intenta guardar y el cortafuegos no es capaz de bloquear la descarga o ejecución del mismo, el ciberdelincuente habría logrado su objetivo: infectar el sistema del receptor del mensaje mediante dichos archivos maliciosos. En la siguiente captura se puede apreciar cómo los archivos que contiene aparentan ser ficheros normales en .pdf, pero realmente tienen una extensión .lnk.



Microsoft vincula ataques similares de tipo phishing a Storm-0324. Pese a que existen multitud de similitudes en el modus operandi, no existe la certeza de que se trate de los mismos autores.

Listado de referencias

Malware distributor Storm-0324 facilitates ransomware access | Microsoft Security

LINK DE LA NOTICIA

Fuente: incibe.es