	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°160	Fecha: 07-07-2023
		Página: 9 de 27

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	La herramienta TeamsPhisher aprovecha los equipos de Microsoft para implementar malware		
Tipo de Ataque	Ransonware	Abreviatura	Ransonware
Medios de propagación	Correo electrónico, redes sociales, entre otros.		
Código de familia	C	Código de Sub familia	c01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

El 06 de julio del 2023, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se ha tomado conocimiento de una nueva herramienta disponible en GitHub que puede permitir a los atacantes hacer un mal uso de una vulnerabilidad que fue recientemente revelada en Microsoft Teams y enviar automáticamente archivos maliciosos a los sistemas de los usuarios.

2. DETALLES:

Los investigadores de Microsoft Incident Response investigaron recientemente una intrusión en la que la rápida progresión del ataque del actor de amenazas causó importantes interrupciones para la organización víctima en solo cinco días.

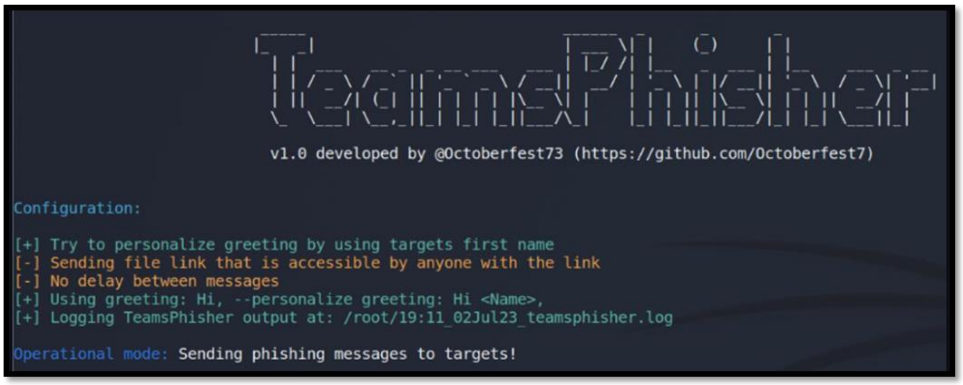
La herramienta, denominada TeamsPhisher, funciona sin problemas en entornos que permiten la comunicación entre usuarios internos y externos de Teams.

A. Modo de operación

- TeamsPhisher es una herramienta basada en Python que proporciona un ataque totalmente automatizado.
- La herramienta primero comprueba un usuario de Teams y verifica que el usuario puede recibir mensajes externos.
- Luego crea un nuevo hilo con el usuario de destino y envía un mensaje con un enlace adjunto de SharePoint.
- Este nuevo hilo aparece en la interfaz de Teams del remitente para la interacción manual y en última instancia inicia el ataque.
- TeamsPhisher busca aprovechar lo mejor de todos estos proyectos y generar un medio robusto, personalizable y eficiente para que las operaciones autorizadas de Red Teams aprovechen Microsoft Teams para escenarios de phishing para acceso.

B. Enlace de descarga de la herramienta

- https://github.com/Octoberfest7/TeamsPhisher.git



Se cita que TeamsPhisher incluye otras características y argumentos opcionales para refinar el ataque. Estos incluyen el envío de enlaces de archivos seguros que solo puede ver el destinatario previsto, la especificación de un retraso entre las transmisiones de mensajes para eludir la restricción y la modificación de los resultados en un archivo de registro.

TeamsPhisher requiere que los usuarios tengan una cuenta de Microsoft Business (a diferencia de una personal, por ejemplo, @hotmail, @Outlook, etc.) con una licencia válida de Teams y SharePoint.

Esto significa que necesitará un arrendatario de AAD y al menos un usuario con la licencia correspondiente. En el momento de la publicación, hay algunas licencias de prueba gratuitas disponibles en el centro de licencias de AAD que cumplen con los requisitos de esta herramienta.

En cuanto a los requisitos locales, recomiendo actualizar a la última versión de Python3. También necesitará la biblioteca de autenticación de Microsoft.

3. RECOMENDACIONES:

- Actualizar el sistema operativo y software instalados en tu equipo o dispositivo, esto evitará que aprovechen las vulnerabilidades que pudiesen tener para evitar la propagación de amenazas, como la instalación de virus, spam, etc.
- Verificar que los sitios web que se visitan tengan “candado de seguridad” al inicio de la dirección URL.
- Tener cuidado al abrir archivos desconocidos o realizar transferencias de archivos.
- Cambiar las contraseñas periódicamente a su vez se sugiere evitar que estas se relacionen con información personal y que se repitan en diferentes cuentas.
- Instalar soluciones de antivirus, firewall y anti spam, esto mitigará los riesgos y/o propagación de amenazas que se puedan encontrar en internet.

Fuente de Información:	hxxps://cyware.com/news/teamsphisher-tool-exploits-microsoft-teams-to-deploy-malware-325a6034