Microsoft reveló este jueves una *«extensa serie de campañas de phishing de credenciales»,* que aprovecha un kit de phishing personalizado que unía componentes de al menos cinco diferentes kits de amplia circulación, con el objetivo de desviar la información de inicio de sesión del usuario.

El equipo de inteligencia de amenazas de Microsoft 365 Defender de la compañía, que detectó las primeras instancias de la herramienta en la naturaleza en diciembre de 2020, denominó la infraestructura de ataque de copiar y pegar como TodayZoo.

> *«La abundancia de kits de phishing y otras herramientas disponibles para la venta o el alquiler hace que sea fácil para un atacante lobo solitario elegir las mejores características de estos kits. Ellos juntan estas funcionalidades en un kit personalizado e intentan cosechar todos los beneficios para ellos mismos. Tal es el caso de TodayZoo»,* dijeron los investigadores.

Los kits de phishing, que por lo general se venden como pagos únicos en foros clandestinos, son archivos empaquetados que contienen imágenes, scripts y páginas HTML que permiten a un actor de amenazas configurar correos electrónicos y páginas de phishing, usándolos como señuelos para recolectar y transmitir credenciales a un servidor controlado por el atacante.

La campaña de phishing TodayZoo no es distinta en el sentido de que los correos electrónicos del remitente se hacen pasar por Microsoft, afirmando ser un restablecimiento de contraseña o notificaciones de fax y escáner, para redirigir a las víctimas a las páginas de recolección de credenciales.

El kit de phishing se destaca en su improvisación a partir de fragmentos de código extraídos de otros kits. *«Algunos están disponibles para la venta a través de vendedores de estafas de acceso público o son reutilizados y reempaquetados por otros vendedores de kits».*

Específicamente, gran parte del marco parece haber sido extraído de otro kit, conocido como DanceVida, mientras que los componentes relacionados con la imitación y la ofuscación se superponen significativamente con el código de al menos otros cinco kits de phishing como Botssoft, FLCFood, Office-RD117, WikiRed y Zenfo. A pesar de depender de módulos reciclados, TodayZoo se desvía de DanceVida en el componente de recolección de credenciales al reemplazar la funcionalidad original con su propia lógica de exfiltración.

En todo caso, la «*característica del monstruo de Frankenstein de TodayZoo*» ilustra diversas formas en que los actores de amenazas aprovechan los kits de phishing con fines oscuros, ya sea alquilándolos a proveedores de phishing como servicio (PhaaS) o construyendo sus propias variantes desde cero para adaptarse a sus objetivos.

> *«Esta investigación demuestra además que la mayoría de los kits de phishing observados o disponibles en la actualidad se basan en un grupo más pequeño de 'familias de kits más grandes'. Si bien esta tendencia se ha observado anteriormente, sigue siendo la norma, dado que los kits de phishing que hemos visto comparten grandes cantidades de código entre ellos»,* dice el análisis de Microsoft.