CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Campaña de Phishing

Fecha: 03/08/2022

Problemática: Campaña masiva de phishing dirigida a usuarios del servicio de correo electrónico de Microsoft Outlook

Correlativo: AA-0006

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

El grupo de ciberseguridad “Zscaler ThreatLabz” alerta sobre la campaña masiva de phishing dirigida a los usuarios empresariales del servicio de correo electrónico de Microsoft Outlook.

SITUACIÓN

Los ciberdelincuentes pueden intentar posicionarse entre dos o más dispositivos en red utilizando una técnica de adversario en el medio AiTM Adversary-in-the-middle para respaldar comportamientos de seguimiento como Network Sniffing o Transmitted Data Manipulation . Al abusar de las características de los protocolos de red comunes que pueden determinar el flujo del tráfico de la red, los ciberdelincuentes pueden obligar a un dispositivo a comunicarse a través de un sistema controlado por el adversario para que puedan recopilar información o realizar acciones adicionales.

Los ciberdelincuentes pueden configurar una posición similar a AiTM para evitar que el tráfico fluya hacia el destino apropiado, potencialmente para perjudicar las defensas y/o en apoyo de una denegación de servicio de red.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	Preventiva

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	Alta	Bajo	Bajo

RECOMENDACIONES

Ante esta alerta se dan las siguientes recomendaciones para mitigar este tipo de ataques:

1. Deshabilite los protocolos de red heredados que pueden usarse para interceptar el tráfico de red
2. Asegúrese de que todo el tráfico cableado y/o inalámbrico esté encriptado adecuadamente. Utilice las mejores prácticas para los protocolos de autenticación, como Kerberos, y asegúrese de que el tráfico web que pueda contener credenciales esté protegido por SSL/TLS.
3. Utilice dispositivos de red y software de seguridad basado en host para bloquear el tráfico de red que no es necesario dentro del entorno
4. Limite el acceso a la infraestructura de red y los recursos que se pueden usar para remodelar el tráfico o producir condiciones AiTM.
5. Los sistemas de detección y prevención de intrusiones en la red que pueden identificar patrones de tráfico indicativos de actividad AiTM
6. La segmentación de la red se puede utilizar para aislar los componentes de la infraestructura que no requieren un amplio acceso a la red.

DICCIONARIO DE DATOS

1. AiTM (Adversary-in-the-middle): Técnica utilizada por ciberdelincuentes para interceptar comunicación entre dos sistemas.
2. Phishing: Tecnología que se utiliza como puente entre el origen (un ordenador) y el destino de una solicitud (Internet)
3. Ciberdelincuente: Persona que realiza actividades delictivas en internet como robar información, acceder a redes privadas, estafas entre otros.
4. Network Sniffing: Monitorea el tráfico de la red en busca de información (por ejemplo, de dónde proviene, qué dispositivo, el protocolo utilizado, etc

REFERENCIAS

1. https://www.microsoft.com/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/
2. https://www.zscaler.com/blogs/security-research/large-scale-aitm-attack-targeting-enterprise-users-microsoft-email-services
3. https://attack.mitre.org/techniques/T1557/

ÁREA PARA DEFINICIONES

*La información contenida en este documento y sus anexos son CONFIDENCIALES y puede contener información PRIVILEGIADA para uso exclusivo de su destinatario intencional. Si lo ha recibido por ERROR o si no es su destinatario intencional, favor NOTIFIQUELO al remitente y bórrelo inmediatamente de su sistema, así como todos los adjuntos y las COPIAS generadas. La distribución, copia u otro uso de este mensaje por terceras personas está PROHIBIDA y puede resultar ilegal.

*La presente herramienta tiene aplicación práctica derivado a un proceso previo de análisis con base al contexto y la situación del evento, sin embargo, se aclara que el presente sirve como guía y marco de referencia.