CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Exfiltrasión de credenciales de acceso

Fecha: 23/08/2022

Problemática: Técnicas de Phishing de voz sofisticado (Vishing)

Correlativo: AA-0013

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Cisco Security Incident Response (CSIRT) y el grupo inteligente de ciberseguridad de la compañía Cisco Talos dio a conocer que un grupo de ciberdelincuentes llevaron a cabo una serie de sofisticados ataques de phishing de voz bajo la apariencia de varias organizaciones de confianza, intentando convencer a la víctima de que aceptara las notificaciones push de autenticación multifactor (MFA).

SITUACIÓN

El acceso inicial a Cisco VPN se logró mediante el compromiso exitoso de la cuenta personal de Google de un empleado de Cisco. El usuario había habilitado la sincronización de contraseñas a través de Google Chrome y había almacenado sus credenciales de Cisco en su navegador, lo que permitió que esa información se sincronizara con su cuenta de Google. Después de obtener las credenciales del usuario, el atacante intentó eludir la autenticación multifactor (MFA) utilizando una variedad de técnicas, incluido el phishing de voz (también conocido como "vishing") y la fatiga de MFA, una serie de sofisticados ataques de phishing de voz para eludir las notificaciones automáticas de autenticación multifactor para acceder a la VPN del empleado de Cisco.

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	Alta	Alta

RECOMENDACIONES

1. Cisco aconseja reforzar la autenticación multifactor MFA, la verificación de dispositivos y la segmentación de la red para mitigar los riesgos.
2. Dada la habilidad demostrada por el ciberdelincuente en el uso de una amplia gama de técnicas para obtener el acceso inicial, la educación del usuario es también una parte clave para contrarrestar las técnicas de evasión de MFA.
3. Igualmente importante para la implantación de la MFA es garantizar que los empleados sepan qué hacer y cómo responder si reciben solicitudes push erróneas en sus respectivos teléfonos.

DICCIONARIO DE DATOS

1. Endpoint Detection and Response-EDR (Detección y Respuesta de Amenazas de Puntos Finales): Tecnología de ciberseguridad que monitorea continuamente un "punto final" para mitigar amenazas cibernéticas maliciosas
2. Extended Detection and Response - XDR (Detección y Respuesta Extendidas): Tecnología de ciberseguridad que monitorea y mitiga las amenazas de ciberseguridad
3. Cifrado: Operación o función matemática utilizada en combinación con una clave que se aplica a un texto en claro y permite obtener un texto cifrado (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida.
4. Malware: Es un programa malicioso que tiene como característica principal su alto grado de dispersabilidad, es decir, lo rápidamente que se propaga.
5. IDS (Intrusion Detection System): Un sistema de detección de intrusos es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red.
6. Virtual Private Network Red privada virtual (VPN): Tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet.
7. Remote Desktop Protocol (RDP) (Protocolo de Escritorio Remoto): Protocolo desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre una terminal y un servidor Windows.

REFERENCIAS

https://blog.talosintelligence.com/2022/08/recent-cyber-attack.html?m=1
https://attack.mitre.org/techniques/T1566/
https://attack.mitre.org/techniques/T1078/
https://attack.mitre.org/techniques/T1569/002/
https://attack.mitre.org/techniques/T1136/001/
https://attack.mitre.org/techniques/T1573/002/
https://attack.mitre.org/techniques/T1546/012/
https://attack.mitre.org/techniques/T1070/
https://attack.mitre.org/techniques/T1070/001/
https://attack.mitre.org/techniques/T1036/005/
https://attack.mitre.org/techniques/T1098/005/
https://attack.mitre.org/techniques/T1562/004/
https://attack.mitre.org/techniques/T1003/001/
https://attack.mitre.org/techniques/T1003/003/
https://attack.mitre.org/techniques/T1021/
https://attack.mitre.org/techniques/T1071/001/
https://attack.mitre.org/techniques/T1219/
https://attack.mitre.org/techniques/T1112/
https://attack.mitre.org/techniques/T1003/002/
https://attack.mitre.org/techniques/T1621/
https://attack.mitre.org/techniques/T1012/

ÁREA PARA DEFINICIONES