Los métodos más utilizados por cibercriminales para lograr acceso a redes corporativas

Agencias de ciberseguridad de Estados Unidos, Canadá, Nueva Zelanda, Países Bajos y Reino Unido elaboraron de manera conjunta un reporte con las debilidades que más comúnmente son explotadas por atacantes en su intento de acceder a los sistemas de una organización. ESET, compañía líder en detección proactiva de amenazas, analiza los 10 vectores de acceso inicial más utilizados por actores maliciosos y acerca recomendaciones para minimizar los riesgos.

Con respecto a las fallas de seguridad en los controles de seguridad, configuraciones débiles o inseguras y malas prácticas que explotan los cibercriminales, las 10 más comunes son:

1.- No habilitar la autenticación multifactor: La autenticación multifactor es clave para prevenir el secuestro de cuentas. De hecho, varios estudios han demostrado cuán efectiva es esta capa de seguridad adicional a la hora de evitar que atacantes logren exitosamente el acceso a través de credenciales robadas.

2.- Asignar accesos y permisos de forma incorrecta: La incorrecta gestión de accesos y permisos puede permitir que alguien interno lleve adelante acciones que suponen algún riesgo para la organización por tener accesos y permisos innecesarios a información sensible.

3.- Uso de software desactualizado: En muchos casos los atacantes rápidamente tienen acceso a exploits a pocos días de que se dé a conocer la existencia de una vulnerabilidad, pero también ocurre que muchas organizaciones utilizan software desactualizado expuesto a vulnerabilidades de larga data.

4.- Uso de las credenciales de acceso que vienen por defecto: Mantener el mismo nombre de usuario y contraseña que vienen por defecto en software y hardware que compramos es un riesgo muy elevado, ya que ofrece a los atacantes una forma fácil de acceder remotamente a los sistemas a través de estas soluciones.

5.- Falta de controles en servicios de acceso remoto: Los atacantes, como grupos de ransomware, suelen aprovechar configuraciones inseguras o vulnerabilidades sin parchear en soluciones para el acceso remoto a las redes de una organización, como las soluciones VPN.

6.- Uso de contraseñas débiles: Los actores de amenazas utilizan distintos métodos para obtener credenciales de acceso válidas y aprovecharlas para obtener acceso inicial a los sistemas de una organización. Desde ataques de fuerza bruta, a la compra de credenciales robadas en foros clandestinos, entre otras.

7.- Servicios en la nube sin protección: El crecimiento de la demanda y adopción de servicios en la nube, sobre todo con el trabajo remoto e híbrido, también atrajo el interés de los actores de amenazas que buscan la forma de aprovechar errores de configuración y vulnerabilidades en esta superficie de ataque para el robo de información.

8.- Servicios expuestos a internet mal configurados o puertos abiertos: Se utilizan herramientas para descubrir puertos abiertos de servicios expuestos a Internet que pueden permitir acceder a la red de una organización, como pueden ser servicios RDP o el protocolo Server Message Block (SMB).

9.- Error al detectar un correo de phishing: La falta de capacitación puede elevar el riesgo de que los empleados puedan no ser capaces de detectar un correo de phishing malicioso y esto deriva en mayores probabilidades de que la organización se convierta en víctima. Los atacantes suelen recurrir a esta técnica de larga data que sigue siendo efectiva por la falta de concientización y educación en temas de seguridad.

10.- Respuesta pobre de productos de seguridad instalados: Muchas veces los actores de amenazas logran evadir los controles de seguridad que establecen los productos de seguridad instalados en el equipo comprometido y de esta manera logran llevar adelante sus ataques de manera efectiva sin ser detectados. Existen distintas alternativas que utilizan los cibercriminales para lograr esto, como el uso de droppers o de fileless malware.

"Además de repasar las debilidades y/o fallas de seguridad más comunes, es importante mencionar cuáles son las técnicas más utilizadas por los cibercriminales para aprovechar esas debilidades y obtener acceso a los sistemas de una organización. Dentro de estas se encuentran: la explotación de aplicaciones públicas en Internet, los servicios de acceso remoto expuestos a Internet, el phishing, la explotación de relaciones de confianza, y las cuentas válidas. Conocer los riesgos nos permite estar mejor preparados para así evitar ser víctimas de ataques", comenta **Camilo Gutiérrez Amaya,** Jefe del Laboratorio de Investigación de ESET Latinoamérica.

En cuanto a las **recomendaciones** para que las organizaciones puedan minimizar las posibilidades de que actores maliciosos logren acceso a sus sistemas, algunas de las prácticas sugeridas son:

- Adoptar el modelo de seguridad zero trust
- Limitar la posibilidad de que se pueda acceder de forma remota a una cuenta de administrador
- Controlar los permisos y accesos asignados a los diferentes datos y servicios, lo que incluye aplicar el principio de menor privilegio para que cada empleado tenga acceso a la información que necesita para realizar su tarea y nada más
- Establecer cambios de contraseña
- Gestionar procesos de entrada y salida de empleados y cambios de posición internos
- Verificar que ningún equipo tiene el puerto RDP abierto
- Implementar la autenticación multifactor
- Modificar o inhabilitar nombres de usuario y contraseñas que vienen por defecto
- Monitorear el uso de credenciales comprometidas en los sistemas internos

- Gestión centralizada de logs
- Uso de soluciones antimalware

Para conocer más sobre seguridad informática ingrese al portal de noticias de ESET: https://www.welivesecurity.com/la-es/2022/07/07/estafas-comunes-facebook-marketplace/