Investigadores de seguridad afirman haber encontrado evidencia de que un grupo de piratería vinculado al gobierno chino ha pasado por alto la autenticación de dos factores (2FA) en una ola de ataques cibernéticos.

Los ataques se atribuyeron a un grupo que la industria de la seguridad cibernética está rastreando como APT20, que se cree que opera a instancias del gobierno de Beijing, según confirmó la firma holandesa de seguridad cibernética, Fox-IT, en un informe publicado la semana pasada.

Los objetivos principales del grupo eran entidades gubernamentales y proveedores de servicios gestionados (MSP). Las entidades gubernamentales y los MSP estaban activos en campos como la aviación, atención médica, finanzas, seguros, energía e incluso, las cerraduras físicas.

El informe de Fox-IT especifica que el ataque de APT20 se remonta a 2011, pero los investigadores perdieron el rastro de las operaciones del grupo en 2016-2017, cuando cambiaron su modo de operación.

Según los investigadores, los hackers utilizaron servidores web como punto de entrada inicial a los sistemas de un objetivo, con un enfoque particular en JBoss, una plataforma de aplicaciones empresariales que a menudo se encuentra en grandes redes corporativas y gubernamentales.

APT20 utilizó vulnerabilidades para obtener acceso a estos servidores, instalar shells web y luego propagarse lateralmente por medio de los sistemas internos de las víctimas.

Mientras Fox-IT realizaba sus investigaciones, encontró que el grupo arrojó contraseñas y buscó cuentas de administrador, para maximizar su acceso. Una preocupación principal era obtener las credenciales de VPN, para que los piratas informáticos pudieran escalar el acceso a áreas más seguras de la infraestructura de la víctima, o utilizar las cuentas de VPN como puertas traseras más estables.

Fox-IT dijo que a pesar de lo que parece ser una actividad de piratería muy prodigiosa en los últimos dos años, *«en general, el actor ha podido permanecer fuera del radar».*

Esto gracias al uso de herramientas legítimas que ya estaban instaladas en dispositivos pirateados, en lugar de descargar su propio malware personalizado, que podría haber sido detectado por el software de seguridad local.

Sin embargo, eso no fue lo más notable. Los análisis de Fox-IT revelaron que se encontró evidencia de que los hackers se conectaron a cuentas VPN protegidas por 2FA.

Aunque no está claro cómo lograron eso, el equipo de investigadores propuso su teoría. Afirmaron que APT20 robó un token de software RSA SecurID de un sistema hackeado, que el actor chino usó en sus computadoras para generar códigos válidos de un solo uso y omitir 2FA a voluntad.

Normalmente esto no sería posible. Para utilizar uno de estos tokens de software, el usuario necesita conectar un dispositivo físico a su computadora. El dispositivo y el token de software generan un código 2FA válido. Si falta el dispositivo, el software RSA SecurID generaría un error.

Los investigadores explican cómo los piratas informáticos podrían haber solucionado ese problema:

> *«El token de software se genera para un sistema específico, pero, por su puesto, este valor específico del sistema podría ser fácilmente recuperado por el actor al tener acceso al sistema de la víctima. Como resultado, el actor en realidad no necesita pasar por el problema de obtener el valor específico del sistema de la víctima, porque este valor específico solo se verifica al importar el seed de Token SecurID, y no tiene relación con la semilla utilizada para generar dos tokens reales. Esto significa que el actor puede simplemente parchear la verificación que analiza el token importado y generado para el sistema, y no necesita molestarse en robar el*

> *valor específico del sistema».*
>
> *«En resumen, todo lo que el actor tiene que hacer para usar los códigos de autenticación de 2 factores es robar un token de software RSA SecurID y parchear una instrucción, lo que resulta en la generación de tokens válidos».*

Operación WOCAO

Fox-IT informó que pudo investigar los ataques de APT20 ya que fueron llamados por una de las compañías pirateadas para ayudar a investigar y responder a los ataques cibernéticos.

Se puede encontrar más información al respecto en el informe titulado *«Operación Wocao».*

La compañía dijo que adoptó el nombre Wocao después de una respuesta de los hackers chinos luego de que fueron detectados y expulsados de la red de una víctima.

En la captura de pantalla, se puede ver a APT20 tratando de conectarse a un shell web, ahora eliminado, que instalaron en la red de la víctima.

Los hackers intentan ejecutar distintos comandos de Windows. Cuando los comandos no se ejecutan, los hackers de APT20 entienden que han sido detectados y expulsados de la red, y escriben un último comando con frustración: wocao, que es la jerga china para *«mierda» o «maldición».*