beazley

Cómo un ataque de phishing fue parado en seco

mayo 02, 2024

Los empleados de una gran empresa de comunicaciones fueron objeto de una campaña de phishing.

Los mensajes de texto enviados a sus teléfonos personales contenían un enlace a un sitio malicioso que parecía ser del empleador, pero que estaba diseñado para recopilar el nombre de usuario, la contraseña y el código de segundo factor.

Inmediatamente después de que su equipo de respuesta a incidentes fuera notificado de la campaña, su centro de operaciones de seguridad abrió una investigación, que reveló que 15 empleados habían introducido sus credenciales en el sitio web malicioso. Utilizando las credenciales comprometidas, el hacker accedió a herramientas internas y restableció las contraseñas de correo electrónico de 27 cuentas de correo electrónico de clientes.

Se bloquearon y modificaron las credenciales de todos los empleados comprometidos y se restablecieron las contraseñas de los 27 clientes afectados para impedir que nadie pudiera seguir accediendo a las cuentas.

beazley