appgate

CASE STUDY

BANCO MULTINACIONAL EMPLEA DETECCIÓN PROACTIVA DE MALWARE PARA DETENER ATAQUES DE FRAUDE Y PROTEGER SUS USUARIOS CONTRA LOS TROYANOS ZEUS PANDA Y MARCHER

RESUMEN

Problema de ataques de malware contra sus usuarios. Es así como Appgate descubrió una campaña que atacaba activamente a la institución a través de dos reconocidos troyanos bancarios: Zeus Panda y Marcher.

Detect Safe Browsing (DSB) Framework de Appgate se integra en todas las plataformas móviles y online. La versión Clientless de la solución analiza las plataformas online del banco para revisar si han sido alteradas. Por su parte, la versión Client detecta la presencia de malware financiero en los dispositivos del usuario y bloquea la transmisión de las credenciales robadas a los servidores de comando y control de los cibercriminales. Finalmente, DSB Mobile se integra en la aplicación móvil de la institución para brindar una conexión segura entre la plataforma bancaria y el dispositivo del usuario.

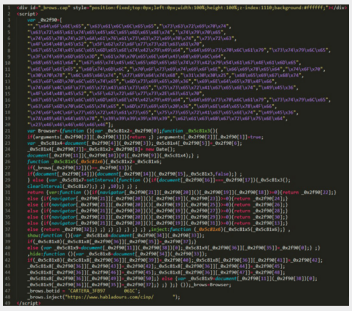
EL BANCO EN LA MIRA DE SOFISTICADOS TROYANOS

El malware Zeus Panda que encontramos atacando al banco fue particularmente potente debido a su habilidad de capturar, no solo las credenciales de acceso del usuario, sino también los códigos de autenticación de segundo factor (2FA). Tal captura depende de si el objetivo del malware es un cliente particular o corporativo.

En el caso de los clientes corporativos infectados con Zeus Panda, el troyano inyecta un script malicioso en la página de inicio de sesión del banco, el cual añade un campo adicional para la contraseña OTP que funciona como 2FA. El usuario recibe su contraseña y la ingresa en el nuevo campo, siendo capturada por los atacantes junto con las credenciales de ingreso.

Por otra parte, los usuarios particulares que intentan ingresar a sus cuentas bancarias desde dispositivos infectados son desviados por el malware hacia una página falsa en donde se les pide descargar una aplicación móvil (el troyano Marcher). Si el usuario continúa con el proceso, los cibercriminales obtienen la habilidad de interceptar el código de autenticación OTP enviado vía SMS.

Zeus Panda espera en silencio en el equipo infectado hasta que el usuario intenta ingresar a la página del banco y, cuando lo hace, inyecta su código malicioso, comprometiendo lo que el usuario ve en lo que sería la página legítima.



El JavaScript malicioso, en morado, que fue inyectado en la página de ingreso del banco cuando un usuario infectado intentó iniciar sesión.

LA NECESIDAD

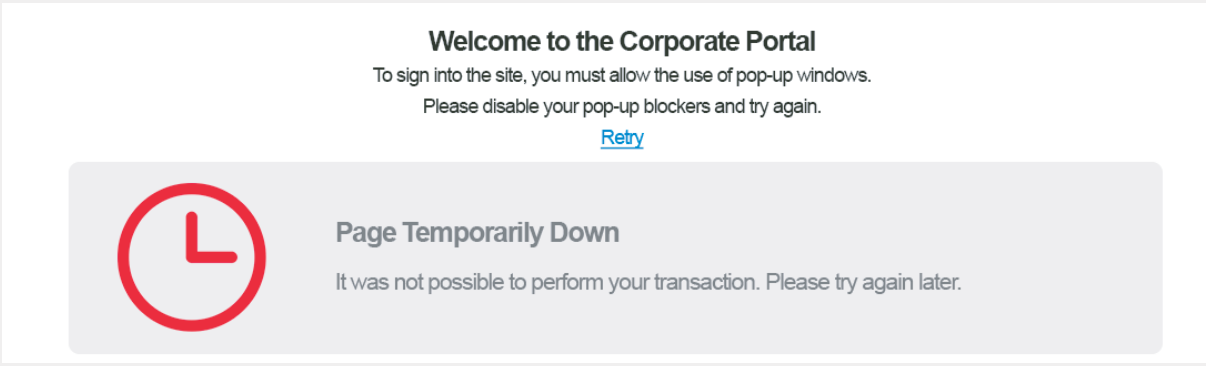
En un ataque coordinado, los defraudadores atacaron a los clientes de una institución financiera con dos tipos diferentes de malware. El banco necesitaba detectar y mitigar rápidamente las amenazas y prevenir que hubiera víctimas y robo de fondos.

SOLUCIÓN IMPLEMENTADA:

DSB Framework protege la conexión entre la plataforma del banco y el dispositivo del usuario de manera que las transacciones se realicen de forma segura, incluso en equipos infectados. La solución también puede identificar y neutralizar cualquier ataque presente en computadores, celulares y tabletas. Además, DSB Framework detecta si algún código malicioso ha sido inyectado en las páginas de inicio de sesión del banco, ayudando a proteger toda la base de clientes de la institución financiera, sin importar en qué dispositivo realizan sus transacciones. La combinación de estas habilidades de detección y conexión segura les quita a los troyanos Zeus Panda y Marcher el poder de ejecutar robos financieros.

LOS BENEFICIOS

La estrategia de defensa múltiple detecta y neutraliza ataques sofisticados de cualquier clase, incluyendo troyanos bancarios y ataques de Man-in-the-Middle, manteniendo protegidas las cuentas de los usuarios contra ingresos no autorizados.



PÁGINA MOSTRADA DESPUÉS DE QUE EL TROYANO ZEUS PANDA RECOLECTA CON ÉXITO LAS CREDENCIALES DE ACCESO Y OTP DE UN CLIENTE CORPORATIVO.

DE ZEUS PANDA A MARCHER

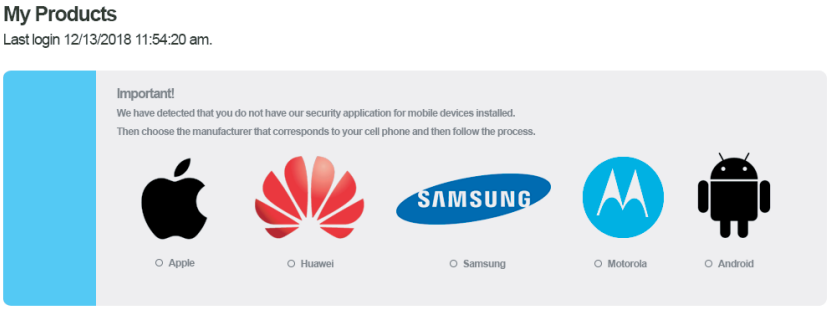
El comportamiento del malware después de la inyección depende de qué tipo de cliente bancario es comprometido. El proceso de 2FA para clientes corporativos es mucho más seguro que el ofrecido a usuarios particulares, por lo cual es mucho más difícil para el troyano ganar acceso a los códigos. Para sortear este obstáculo, el malware sencillamente solicita el código de 2FA al usuario. Al ver que todo parece normal, el usuario ingresa la contraseña OTP que recibió en un mensaje SMS. La víctima es luego redirigida a una pantalla que dice: "Página Inactiva Temporalmente". Esto es una cortina de humo diseñada para confundir al usuario.

Para los clientes particulares que son engañados para revelar sus credenciales de acceso, una pantalla adicional es desplegada con instrucciones para que descarguen lo que aparentemente es la "más reciente aplicación de seguridad móvil" del banco.

Los usuarios que crean que su banco ha desplegado una nueva medida de seguridad para mantenerlos a salvo (a pesar de no haber recibido una notificación previa), posiblemente sean los que continúen con el proceso.

Luego, los usuarios son dirigidos a una página que les pide descargar el software malicioso disfrazado de aplicación de seguridad (desde un enlace proporcionado por el cibercriminal). Después de eso, el dispositivo estaría infectado con el troyano móvil Marcher.

Ahora que Marcher entró al juego, el cibercriminal está listo para capturar el 2FA entregado por el banco sin que el usuario lo sepa. El hacker ha conseguido todo lo necesario para robar los fondos del cliente a voluntad.



Troyano Zeus Panda pidiendo al cliente bancario que descargue "la última aplicación de seguridad", la cual en realidad es el troyano de banca móvil Marcher

CÓMO LOGRAMOS AYUDAR AL BANCO A MITIGAR LAS AMENAZAS

Nuestra solución Detect Safe Browsing (DSB) Clientless detectó la presencia de la inyección de malware en la página transaccional cuando un usuario, cuyo dispositivo había sido infectado por el malware, visitó el sitio. Después, DSB entregó evidencia a través de una captura de pantalla obtenida gracias a la función Malware Snapshot, la cual incluía el nombre de usuario de la víctima. Esto le permitió a la institución tomar acciones inmediatas para mitigar el ataque, incluyendo el bloqueo automático de cualquier sesión infectada y el contacto con las primeras víctimas para investigar a fondo los vectores de infección y las muestras de malware usados en el ataque.

Nuestra solución de navegación segura, DSB Mobile, protege todas las comunicaciones entre una institución financiera y sus clientes a través de la aplicación bancaria, es decir, las aplicaciones maliciosas como Marcher no podrán capturar información ilegalmente. De hecho, la intercepción de mensajes SMS por parte del malware sirve como recordatorio de que los entes regulatorios del mundo recomiendan la inhabilitación de estos mensajes como segundo factor de autenticación debido a situaciones como estas. Además, DSB Mobile protege contra otras técnicas de robo de credenciales como aplicaciones falsas, ataques de superposición, keyloggers o pharming. En el caso descrito anteriormente, las aplicaciones maliciosas usadas en el ataque fueron agregadas en la lista negra de manera que ningún otro usuario las descargue.

Finalmente, los usuarios que descargaron e instalaron DSB Client en sus computadores fueron protegidos automáticamente gracias a la incorporación de la información del ataque desde nuestra base de datos. DSB Client fue capaz de neutralizar efectivamente a Zeus Panda y demás troyanos al suprimir la habilidad del malware de comunicarse con la estructura de comando y control (C&C) del atacante mientras los agentes de Centro de Operaciones de Seguridad (SOC) retiraban los servidores C&C de Internet.

En Appgate hemos estado observando de cerca la evolución del troyano Zeus Panda para saber cuándo los cibercriminales intenten desarrollar o reensamblar el malware o sus servidores C&C y así reaccionar según sea el caso. Hacer esto efectivamente elimina cualquier amenaza futura hasta el punto en que deja de ser rentable para el atacante siquiera intentar relanzar el ataque.