Publicado en Madrid el 23/11/2022

Black Friday: el robo de credenciales bancarias se duplica en 2022

Los analistas de Kaspersky han descubierto que el número de ataques a través de troyanos bancarios se ha duplicado en 2022, en comparación con 2021, alcanzando los 20 millones. En el Black Friday en particular, los fraudes utilizan un nuevo tipo de phishing que, por primera vez, explota el concepto 'compra ahora y paga después'. Estas son algunas de las evidencias reflejadas en el informe 'Cómo los clientes son estafados en la campaña Black Friday de 2022', realizado por Kaspersky

Los troyanos bancarios son muy utilizados por los ciberdelincuentes, que hacen su agosto en la temporada de ventas. Cuando el usuario navega por una tienda online, el troyano almacena todos los datos que el cliente introduce en los formularios de la web. Esto supone que los ciberdelincuentes obtienen acceso a la numeración de las tarjetas de crédito o débito, fecha de vencimiento y CVV y las credenciales de inicio de sesión de la víctima. Con esa información, pueden vaciar la cuenta bancaria del usuario, utilizar los datos de la tarjeta para realizar compras o vender los datos en la Dark Web.

Después de una rápida caída en el número de ataques a través de troyanos bancarios en 2021, los ciberdelincuentes han vuelto a este tipo de amenazas con fuerza renovada. En 2022, el número de ataques se ha visto duplicado de enero a noviembre respecto al mismo periodo del año anterior. En ese periodo, las herramientas de Kaspersky han detectado y evitado casi 20 millones de ataques, lo que supone un aumento en las detecciones del 92%. En España, el número de ataques con troyanos bancarios detectados por las herramientas de Kaspersky ha superado los 33 mil.

La temporada de ventas atrae la atención de tiendas y compradores. Es el momento perfecto para los cibercriminales, que no dudan en aprovecharse de la situación en el caso de los clientes online. Estos crean atractivas ofertas de productos gratuitos o a bajo precio que son falsas y caducan pronto, lo que obliga al usuario a ser rápido. Es este factor el que consigue que los ciberdelincuentes logren estafar al usuario, hambriento de productos y que no se detiene a evaluar si el sitio en el que ha ingresado los datos es una página de phishing o el original.

En 2022, los expertos de Kaspersky también encontraron numerosos ejemplos de páginas de phishing que por primera vez se beneficiaban del 'compra ahora, paga después'. Este servicio permite a los clientes dividir el coste de la compra en varias cuotas y sin intereses. Esto atrae a los usuarios, especialmente a los más jóvenes, y son particularmente populares en momentos como el Black Friday. De hecho, la telemetría de Kaspersky también ha registrado 351.800 correos electrónicos que contienen las palabras "Black Friday", una cifra cinco veces mayor que los correos detectados en octubre. Y, en comparación con septiembre, el crecimiento es de más del 437%.

Un ejemplo de esta estafa es el uso indebido de un servicio muy popular denominado Afterpay (Clearpay en Reino Unido e Italia) con 20 millones de usuarios activos en todo el mundo. Los atacantes generan una página que imita la original, engañando a las víctimas para que ingresen la numeración de la tarjeta de crédito y CVV en un formulario falso. Tras conseguir esos datos, los

ciberdelincuentes tratarán de robar la mayor cantidad del dinero posible de la tarjeta.

"El Black Friday, el evento del año en el ámbito de las compras, es un momento caliente no solo para vendedores y compradores, sino también para los estafadores, que pretenden robar la mayor cantidad de dinero posible a los apresurados clientes. El nuevo método que explota los servicios de 'compra ahora, paga después' demuestra que los ciberdelincuentes no cesan en su intención de atacar a las víctimas, y encuentran nuevos métodos para hacerlo. En días normales, el cliente suele descubrir rápidamente que, si el producto es demasiado barato, lo normal es que se trate de una estafa. Sin embargo, durante las rebajas del Black Friday no lo tienen tan claro. Los compradores pierden el nivel de atención y se convierten en un objetivo fácil para los ciberdelincuentes. Por eso es tan importante prestar atención a la web en la que se realiza la compra, tener cuidado con empresas desconocidas y usar una solución de seguridad fiable", asegura Olga Svistunova, experta en seguridad de Kaspersky.

Para disfrutar de lo mejor del Black Friday este año, hay que asegurarse de seguir estos consejos de seguridad:

Proteger todos los dispositivos que se usen para las compras online con una solución de seguridad fiable. No se puede confiar en links o archivos adjuntos recibidos por correo. Verificar dos veces el remitente antes de abrir cualquier cosa.
Revisar dos veces las tiendas online antes de rellenar cualquier formulario: ¿es correcta la URL? ¿Muestra errores de escritura o diseño?
Para proteger los datos y cuentas bancarias, asegurarse de que la página es segura, y que muestra el clásico icono del candado antes de la dirección.
Si se va a comprar algo de una compañía desconocida, revisar los comentarios sobre la misma antes de tomar una decisión.
A pesar de tomar tantas precauciones como sea posible, probablemente no se sepa que algo va mal hasta que veas el estado de la cuenta bancaria. Consultar a través de internet los cargos recibidos y comprobar que son legítimos. Si no es el caso, contactar con el banco para solucionar la situación.

Para saber más sobre las estafas durante el Black Friday, acceder a Securelist.

Datos de contacto:
Mónica Iglesias
690196537

Nota de prensa publicada en: Madrid

Categorías: Hardware Entretenimiento Ciberseguridad