Un grupo de delincuentes cibernéticos conocido por apuntar a sitios web de comercio electrónico, lanzó una *«campaña maliciosa de múltiples etapas»* a inicios del año, diseñada con la intención de distribuir ladrones de información y skimmers de pagos basados en JavaScript.

En un nuevo informe publicado este lunes por la compañía de seguridad cibernética con sede en Singapur, Group-IB, se atribuyó la operación al mismo grupo que ha sido vinculado a un ataque separado dirigido a comerciantes en línea que utilizan malware para robar contraseñas para infectar sus sitios web con FakeSecurity JavaScript-sniffers (Analizadores de JS).

La campaña avanzó en cuatro oleadas, comenzando en febrero y terminando en septiembre, con los operadores confiando en páginas web de phishing especialmente diseñadas y documentos de atracción atados con marcos maliciosos para descargar los ladrones de información de Vidar y Rccoon en los sistemas de las víctimas.

El objetivo final del ataque, según los investigadores, era robar datos de pago y de usuario a través de varios vectores de ataque y herramientas para distribuir malware.

Las páginas web falsas se crearon utilizando el kit de phishing Mephistophilus, que permite a los atacantes crear e implantar páginas de inicio de phishing diseñadas para distribuir malware.

> *«Los atacantes enviaron enlaces a páginas falsas que informaban a las víctimas sobre la falta de un complemento necesario para mostrar el documento correctamente. Si un usuario descargaba el complemento, su computadora estaba infectada con el malware que roba contraseñas»*, explicaron los investigadores de Group-IB en un análisis de tácticas del grupo en noviembre pasado.

Aunque la primera ola de la campaña en febrero y marzo entregó al ladrón de contraseñas de Vidar para interceptar las contraseñas de los navegadores de los usuarios y varias

aplicaciones, las iteraciones posteriores cambiaron al ladrón de Raccoon y AveMaria RAT para cuplir con sus objetivos.

Raccoon, documentado por primera vez por Cybereason el año pasado, cuenta con una amplia gama de capacidades y se comunica con un servidor de comando y control (C2) para desviar datos, incluidas capturas de pantalla, información de tarjetas de crédito, billeteras de criptomonedas, contraseñas de navegador almacenadas, correos electrónicos y detalles del sistema.

Raccoon también es único porque evita el bloqueo de servidores C2 activos al realizar una solicitud a un canal de Telegram («blintick») para recibir la dirección encriptada del servidor C2, además de ofrecer soporte al cliente 24×7 para preguntas de la comunidad y comentarios por medio del servicio de chat.

AveMaria RAT, de igual forma, es capaz de asegurar la persistencia, registrar pulsaciones de teclas, inyectar código malicioso y exfiltrar archivos sensibles, entre otros.

Tanto Vidar como Raccoon se venden como malware como servicio (MaaS) en foros clandestinos. El precio de alquiler para el ladrón Vidar oscila entre 250 y 300 dólares por mes, mientras que el último cuesta 200 dólares al mes.

Junto con las cuatro etapas descritas, Group-IB también observó una fase intermedia entre mayo y septiembre de 2020, durante la cual hasta 20 tiendas en línea se infectaron con un JS-sniffer modificado de la familia FakeSecurity.

La infraestructura utilizada para distribuir a los ladrones de Vidar y Raccoon compartía similitudes con las que almacenaban el código rastreador y recopilaban datos de tarjetas bancarias robadas, lo que llevó a los investigadores a vincular las dos campañas.

El desarrollo es otra señal de que los adversarios están intensificando sus esfuerzos para comprometer los mercados en línea para robar la información de pago de los clientes, aún cuando las agencias de aplicación de la ley trabajan para abordar el delito cibernético.

A inicios de enero, la Interpol, actuando sobre evidencia forense digital de Group-IB, capturó a tres personas asociadas con un grupo llamado *«GetBilling»* como parte de una operación con nombre en código Night Fury para ejecutar una campaña JS-sniffer en Indonesia.