Las plataformas de comercio electrónico en Estados Unidos, Alemania y Francia, fueron atacadas por una nueva forma de malware que se dirige a los servidores Nginx en un intento de enmascarar su presencia y pasar por alto la detección de las soluciones de seguridad.

> *«Este código novedoso se inyecta a sí mismo en una aplicación host de Nginx y es casi invisible. El parásito se utiliza para robar datos de servidores de comercio electrónico, también conocido como Magecart del lado del servidor»*, dijo el equipo de investigación de amenazas de Sansec.

Nginx es un software gratuito y de código abierto, un servidor web que también se puede utilizar como proxy inverso, equilibrador de carga, proxy de correo y caché HTTP. NginRAT, nombre que se le dio al malware avanzado, funciona secuestrando una aplicación Nginx de host para integrarse en el proceso del servidor web.

El troyano de acceso remoto en sí se encarga a través de CronRAT, otra pieza de malware que la compañía de seguridad cibernética reveló la semana pasada afirmando que oculta sus cargas útiles maliciosas en trabajos cron programados para ejecutarse el 31 de febrero, un día calendario inexistente.

Tanto CronRAT como NginRAT están diseñados para proporcionar una vía remota a los servidores comprometidos, y el objetivo de las intrusiones es realizar modificaciones del lado del servidor en los sitios web de comercio electrónico comprometidos de una forma que permita a los atacantes exfiltrar datos mediante formas de pago en línea.

Los ataques, conocidos colectivamente como Magecart o web skimming, son el trabajo de un sindicato de delitos cibernéticos compuesto por docenas de subgrupos que están involucrados en el robo de tarjetas de crédito digitales mediante la explotación de vulnerabilidades de software para obtener acceso al código fuente de un portal en línea e insertar código JavaScript malicioso que extrae los datos que ingresan los compradores en las páginas de pago.

«Los grupos de skimmer están creciendo rápidamente y apuntando a varias plataformas de comercio electrónico utilizando una variedad de formas para pasar desapercibidos», dijeron los investigadores de Zscaler en un análisis de las últimas tendencias de Magecart publicado a inicios de 2021.

> *«Las últimas técnicas incluyen comprometer versiones vulnerables de plataformas de comercio electrónico, alojar scripts skimmer en CDN y servicios en la nube, y usar dominios recién registrados (NRD) léxicamente cercanos a cualquier servicio web legítimo o tienda de comercio electrónic*o específica para alojar scripts skimmer maliciosos».