FireEye detalla fraudes en terminales punto de venta

FireEye, en conjunto con iSight Partners, dieron a conocer las actividades delictivas en materia de ciberseguridad del grupo FIN6, gracias a una serie de investigaciones dirigidas a descubrir el robo y extracción de datos.

Como resultado de sus operaciones de inteligencia, FireEye tiene una visibilidad extensa de las operaciones de FIN6, que incluye la intrusión inicial y la navegación en las redes de las víctimas, hasta la venta de datos extraídos de tarjetas bancarias mediante operaciones en mercados ilegales.

El término FIN se refiere a grupos delincuenciales especializados en delitos cibernéticos financieros. FIN6 es un grupo criminal cibernético especializado en el robo de datos de tarjetas bancarias, obtenidos a partir de terminales punto de venta, para generar ingresos. Entre los sectores más atacados por el grupo destacan el de la hotelería y el de ventas del sector minorista.

Los datos obtenidos se vendieron en un mercado ilegal difícilmente detectable, utilizando una amplia gama de herramientas y tácticas durante sus intrusiones en las redes informáticas de las víctimas.

No está del todo claro cómo afecta a sus víctimas el grupo FIN6. Mandiant encontró que FIN6 ya poseía credenciales válidas para cada red afectada y llevar a cabo sus actividades intrusivas. En un caso se encontraron rastros de un malware denominado GRABNEW en el servidor de la víctima.

Después de localizar sistemas de punto de venta dentro del entorno elegido, el grupo delincuencial extendió otro malware POS (Point of Sale) que se denomina Trinidad.

En este caso, la inteligencia combinada de FireEye, Mandiant y los equipos de inteligencia de iSIGHT pudo no sólo identificar la actividad maliciosa destinada al robo de datos de tarjetas de pago, sino que también proporcionó una visión detallada acerca de las actividades que derivan en la comercialización de los datos robados.