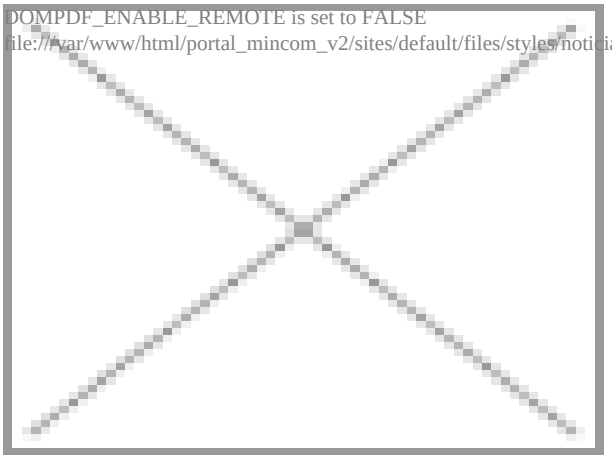

Fuente:
ITConnect
Las empresas que prestan servicios financieros enfrentan amenazas de seguridad con 300% más frecuencia que otras industrias

Raytheon Websense, dio a conocer el Reporte 2015 Financial Services Drill-Down de Websense Security Labs, el cual examina el estado actual de las amenazas cibernéticas y de los ataques que buscan robar datos y que afectan a las instituciones de servicios financieros. Esta investigación revela un alto grado de especialización entre los criminales que atacan a los servicios financieros, una gran inversión en la fase de señuelo, y los ataques específicos y anómalos dirigidos a los objetivos globales en el sector financiero.

“La famosa cita ‘*porque ahí es donde está el dinero’*, atribuida al ladrón de bancos Willie Sutton, se aplica también a los criminales cibernéticos”, señaló Carl Leonard, analista de seguridad de Websense. “Grupos de criminales altamente especializados han estado atacando a esta industria durante años. Al analizar las acciones y los patrones de ataque prominentes y anómalos a esta industria, podemos compartir este conocimiento para proteger los datos y los activos de nuestros clientes de manera más efectiva”.

Mediante el análisis de datos de los patrones de ataques únicos para industrias específicas, los investigadores de Websense lograron obtener nuevos conocimientos sobre los patrones, estructuras y tendencias de los ataques contra el sector de servicios financieros. Los principales hallazgos de este estudio de Websense Security Labs incluyen:

Los Servicios Financieros Sufrieron Incidentes de Seguridad con 300% Más Frecuencia que Otras Industrias: Bajo un bombardeo constante de los criminales cibernéticos, el número de ataques contra el sector financiero supera al volumen promedio de ataques contra otras industrias en una proporción de tres a uno. Además, la sofisticación y la persistencia de los ataques siguen planteando desafíos a los profesionales de la seguridad.

33% de Todos los Ataques en la Etapa de Señuelo Están Dirigidos a los Servicios Financieros: Los hackers están invirtiendo enormes recursos para atacar a los servicios financieros con una cantidad desproporcionada de exploración y señuelos. Uno de cada tres incidentes identificados como señuelos por Websense Security Labs está dirigido a esta industria.

El Robo de Credenciales y el Robo de Datos son los Principales Objetivos de los Criminales: Como se esperaría en el sector de servicios financieros, los ataques para robar datos y credenciales son primordiales para los atacantes. Después de que los investigadores analizaron las principales amenazas que enfrenta esta industria, destacaron que la mayoría tenían algunos elementos para hurtar datos y credenciales. En cuanto al volumen, las principales amenazas vistas en el sector financiero incluyeron a Rerdom, Vawtrack y Geodo. Lo que resulta interesante es que el malware Geodo, con su propio gusano de correo electrónico que roba

credenciales, se ve con 400% más frecuencia en finanzas que en otras industrias.

Los Estafadores Modifican Frecuentemente las Campañas para Burlar las Medidas de Seguridad Bancarias: La ofuscación y el envenenamiento de la optimización de motores de búsqueda siguen teniendo una presencia más importante en los ataques contra los servicios financieros que contra otras industrias. Los patrones de las campañas de ataque cambiaron a un esquema mensual, incluyendo grandes picos en el redireccionamiento malicioso y la ofuscación detectados en una ola de ataques en marzo de 2015. Esto destaca una metodología de ataque diseñada para que les sea más difícil a los encargados de asegurar al sector financiero detectar y analizar las campañas. Además, los criminales cibernéticos mantienen un bombardeo constante de ataques de bajo perfil para mantener ocupados a los profesionales de seguridad que tienen que lidiar con una gran cantidad de distractores mientras que se están realizando ataques dirigidos al mismo tiempo.

Estados Unidos Aloja a la Mayoría de las Amenazas Contra los Servicios Financieros: Además de las fluctuaciones en los tipos de campañas los países desde los cuales se originan los ataques varían considerablemente de un mes a otro. Si bien la mayoría de los sistemas comprometidos que atacan al sector se encuentran en los Estados Unidos, el origen geográfico de campañas específicas varía constantemente. Tan sólo en los últimos cinco años han sido quince los países que se han turnado los cinco primeros lugares desde los cuales se originan los ataques. El reporte aporta más detalles sobre los cambios que los patrones de ataque experimentan cada mes.

Los Servicios Financieros son la Tercera Industria más Afectada por el *Typosquatting* Dirigido: Los investigadores de Websense han observado un aumento en el uso de dominios escritos erróneamente (*typosquatting*) en los ataques dirigidos contra los servicios financieros, y que normalmente se combinan con robustas tácticas de ingeniería social. Al hacer una comparación entre más de 20 industrias, la industria financiera ocupó el tercer lugar en cuanto al número de incidentes de *typosquatting* dirigido. El reporte identifica y describe las principales técnicas de *typosquatting* utilizadas en estos ataques dirigidos.

Asimismo, el reporte examina la posibilidad de que una economía cada vez más global y la adopción de seguros cibernéticos puedan estar entorpeciendo las medidas de seguridad efectivas, y provee más métricas, datos y visualizaciones de los ataques contra los servicios financieros.

Disponible en: http://itclat.com/2015/08/04/amenazas-0001/ [1]

Links
[1] http://itclat.com/2015/08/04/amenazas-0001/