Las amenazas y nuevas técnicas para un ciberataque en 2019

Ataques más difíciles de descubrir para este 2019. Estos serán las tendencias de este año, de acuerdo con expertos.

El 2019 representará un desafío mayor en lo relacionado con ataques cibernéticos debido a que los agentes de amenazas experimentados aplicarán técnicas nuevas y cada vez más complejas, que serán mucho más difíciles de descubrir y atribuir.

"Los agentes de amenazas pasarán a la clandestinidad y bajo el radar para evitar la publicidad y la probabilidad de ser descubiertos. Con suficientes recursos, podrán diversificar los conjuntos de herramientas y prácticas, lo que hará extremadamente difícil detectarlos",

“En 2018, los agentes de amenazas han llevado a nuevos paradigmas (...) Esto provocará un cambio en el panorama cibernético, ya que los agentes de amenazas complejos buscan el silencio y la oscuridad de sus ataques para aumentar la probabilidad de éxito. Este cambio hace que el descubrimiento de operaciones nuevas y sofisticadas a gran escala sea muy improbable, y definitivamente llevará el arte de la detección y la atribución al siguiente nivel".

Predicciones de amenazas para el 2019:

Infectar el *hardware* de la red: Uno de los escenarios más probables es este nuevo enfoque en el que se implementan herramientas especializadas para atacar a víctimas específicas. Permite a los cibercriminales hacer ataques discretos al estilo *botnets,* un conjunto de redes de robots informáticos o *bots* que se ejecutan de forma automática y puede infectar los servidores de forma remota.

Ataques por medio de la cadena de suministro: En los últimos dos años se ha vuelto popular debido a que las empresas trabajan con una gran cantidad de proveedores y es complicado saber qué tan seguros están.

A través de *smartphones*: Seguirán de forma continua y con nuevas formas en las que los atacantes tendrán acceso a los dispositivos de las víctimas. El *malware* móvil ayuda a

ampliar la lista de posibles víctimas en un ataque.

Spear-phising: Los datos obtenidos de diferentes ataques a redes sociales como Facebook, Instagram, Twitter y LinkedIn estarán disponibles en el mercado negro para que cualquiera los adquiera. Las fugas de datos a gran escala ayudarán a los atacantes.

La reacción pública: Las investigaciones de ataques recientes y notables, como los hackeos a Sony Entertainment Network o el ataque contra el Comité Nacional Demócrata, han elevado la exposición pública y judicial de los agentes de amenazas a un nuevo nivel. Esa exposición y la indignación resultante pueden usarse para crear una oleada de opiniones que formen parte del argumento a favor de consecuencias diplomáticas más severas en todo el mundo.

Fuente de información:
https://expansion.mx