Publicado en 28006 el 10/05/2013

El marketing digital, nuevo vehículo para el spam

Para una oleada de spam de contenido pornográfico, con más de 5.000 bots activos, se estaban creando 250 nuevos por día. Para algunas campañas, la vida media de los perfiles fraudulentos es de apenas 45 minutos

Algunas de estas campañas no se limitan sólo a Twitter, sino que están afectando a varias redes sociales, incluso a Facebook

Madrid, 6 de mayo de 2013.- Los fraudes en Twitter están a la orden del día. Con cada noticia de actualidad o evento de magnitud, -el atentado de Boston es uno de los últimos ejemplos-, se crean nuevos bots de spam en esta red social. Algunos de ellos realizan análisis semánticos previos y adaptan los mensajes dependiendo del perfil de la víctima a fin de lograr mayor éxito en su campaña, tal y como destaca Vicente Díaz, analista senior de malware de Kaspersky Lab.

Según Díaz, para mitigar el efecto de estas campañas es posible utilizar técnicas de aprendizaje automático que permiten una tasa de detección de perfiles fraudulentos de hasta el 91% en algunos experimentos.

Twitter suele identificar y neutralizar con facilidad estos bots, pero ellos también se reproducen con la misma facilidad. Para una determinada campaña de spam con contenido pornográfico con más de 5.000 bots activos, se estaban creando 250 nuevos por día. Para algunas campañas, la vida media de los perfiles fraudulentos es de apenas 45 minutos. Estos bots obviamente perjudican a los usuarios y a la misma red social. Es curioso que muchas compañías ofrezcan este servicio como “publicidad social digital”. Podemos ver cómo los mismos perfiles cambian de forma regular, cambiando la descripción del perfil y la foto, con el fin de burlar las medidas de seguridad y adaptarse a la nueva campaña.

La mayoría de los bots usan un diccionario común para los tweets que envían, además de los mensajes spam, con el fin de camuflarse como perfiles legítimos. Pero esto facilita su localización, por lo que tienen que implementar nuevas estrategias para evitar la detección del análisis semántico, como mensajes aleatorios con palabras que este análisis suele ignorar.

Algunas de estas campañas no se limitan sólo a Twitter, sino que están afectando a varias redes sociales, incluso a Facebook. Por ejemplo, la campaña job-deals.com (activa desde principios de abril) ataca principalmente a Twitter, pero podemos ver en Alexa como también los usuarios Facebook resultaron afectados.

“Estos bots no sólo incomodan a los usuarios, sino que además representan una verdadera amenaza

cuando se usan para enviar otras cosas, aparte del spam. Lo que resulta más preocupante es que muchas veces se usan cuentas hackeadas, incrementando notablemente la posibilidad de que los destinatarios activen el enlace, ya que suponen que el remitente es un amigo", señala Díaz. Podemos ver cómo una reciente campaña utilizó esta técnica para capturar cuentas con el siguiente mensaje: "LOL, funny pic of you", tras el enlace estaba sitio malicioso:

Para esta campaña se usaron varios dominios, y volvemos a notar que algunos de ellos también se encontraban en otras redes sociales.

Hay mucho más fraude en las redes sociales; como cuando se usa Twitter para propagar malware, para establecer comunicaciones con programas maliciosos, o para los intereses de hacktivistas, tal y como Kasperky Lab ha detectado recientemente en las elecciones venezolanas.

Datos de contacto:
Everythink

Nota de prensa publicada en: 28006

Categorías: Marketing Ciberseguridad