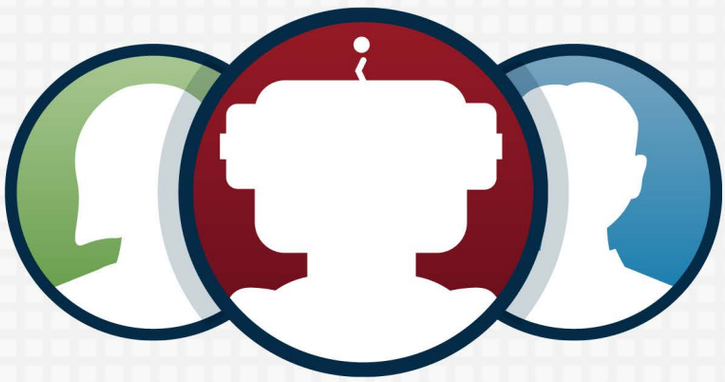
SOCIAL MEDIA BOTS*

Los bots en redes sociales son programas automatizados que simulan interacción humana en las plataformas de redes sociales. A medida que su incidencia y habilidad de imitar el comportamiento humano aumenta, los impactos potenciales, tanto útiles como perjudiciales, se expanden. Visite CISA.gov/MDM para obtener más información.

Los bots en redes sociales utilizan inteligencia artificial, análisis de big data y otros programas o bases de datos para hacerse pasar por usuarios legítimos en las redes sociales. Estos varían según su función y capacidad: algunos son útiles, como los bots de chat y las notificaciones automáticas, pero otros se pueden usar con el fin de manipular a usuarios reales. Cuando se usan inapropiadamente, los bots pueden amplificar la desinformación y distorsionar nuestra percepción acerca de lo que es importante, contaminando o incluso terminando las conversaciones en línea.



Reconocer el comportamiento de los bots puede ayudarnos a responder a sus ataques.

Ataques comunes

Obtención de clics o de reacción "Me gusta" [*Click/ Like Farming*] Los bots incrementan la popularidad de una cuenta al darle reacción "me gusta" o al publicar de nuevo su contenido.

Apropiación de etiquetas [*Secuestro de hashtags*] Los bots atacan a una audiencia aprovechando las etiquetas [los *hashtags*] del grupo (por ejemplo, usando correos basura [*spam*] o enlaces [*links*] maliciosos).

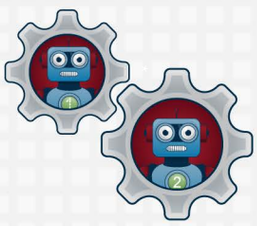
Red de reenvío de publicaciones [*Repost Network*] Los bots coordinados (*"botnet"*) publican nuevamente y de manera instantánea el contenido de un bot "principal".

Bots inactivos o bots durmientes [*Sleepers*] Los bots se despiertan luego de largos períodos de inactividad con el fin de lanzar miles de publicaciones ('posts' en redes sociales) o retuits en poco tiempo.

Campañas artificiales [Operación de *'Astroturfing'*] Los bots comparten contenido de manera coordinada, con el fin de dar una falsa impresión de apoyo u oposición auténticos formulada con la intención de parecer generada por un impulso orgánico común sobre un tema de interés público.

Bombardeos o Asaltos [*Raids*] Los bots se activan de manera coordinada y sobrecargan cuentas específicas y predeterminadas, con correos basura [*spam*].

Los bots pueden ser reconocidos por sus interacciones entre sí y con usuarios reales. A menudo exhiben las siguientes características:

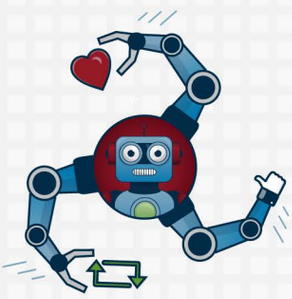


Acciones coordinadas

Los bots a menudo actúan juntos, compartiendo contenido similar al mismo tiempo, o con frecuencia, publicando de nuevo ('reposting') el contenido de unos y otros.

Publicaciones ('posts' en redes sociales') repetitivas y específicas

Los bots a menudo publican contenido idéntico, y utilizan emoticones y puntuación en una forma más distinguible que los usuarios reales.



Altos niveles de actividad

Los bots a menudo tienen niveles de actividad más altos en comparación con el comportamiento típico en redes sociales, publicando frecuentemente y, a menudo, compartiendo contenido sin ninguna opinión.

*Bot es un acortamiento que se refiere a un programa de computadora que actúa como una cuenta automatizada.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés) produjo este gráfico con el fin de resaltar las tácticas utilizadas por las campañas de desinformación que buscan perturbar la vida en los Estados Unidos y la infraestructura crítica que la sostiene. La publicación por parte de CISA de materiales informativos sobre este tema está destinada para conocimiento público y no tiene la intención de restringir, disminuir o denigrar el derecho de cualquier persona a tener, expresar o publicar cualquier opinión o creencia, incluso cuando dichas opiniones o creencias se alinean con las de un gobierno extranjero, se expresan mediante una campaña respaldada por un gobierno extranjero, o disienten de la mayoría

Por favor, tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios - LanguageAccess@cisa.dhs.gov.

Please note: CISA recognizes that language is continually evolving and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov.

SOCIAL MEDIA BOTS*

Las capacidades de los bots en redes sociales han evolucionado desde ayudar con tareas simples en línea hasta asumir comportamientos más complejos que imitan a los usuarios humanos, los cuales son utilizados por actores maliciosos con el fin de manipular nuestras interacciones en línea. Visite CISA.gov/MDM para obtener más información.

Los bots en redes sociales están cada vez más integrados en muchas de nuestras actividades en línea, incluso en ocasiones sin que nos demos cuenta. Hay una gran variedad de bots con funciones y capacidades distintas: Algunos ayudan a automatizar tareas simples, mientras otros bots más avanzados utilizan inteligencia artificial, análisis de big data y otros programas, para imitar a los usuarios humanos. Estos actores maliciosos a veces emplean bots como un componente de esfuerzos coordinados para manipular a los usuarios humanos.

Comprender los diferentes usos de los bots puede ayudarnos a reconocer los intentos de manipulación.

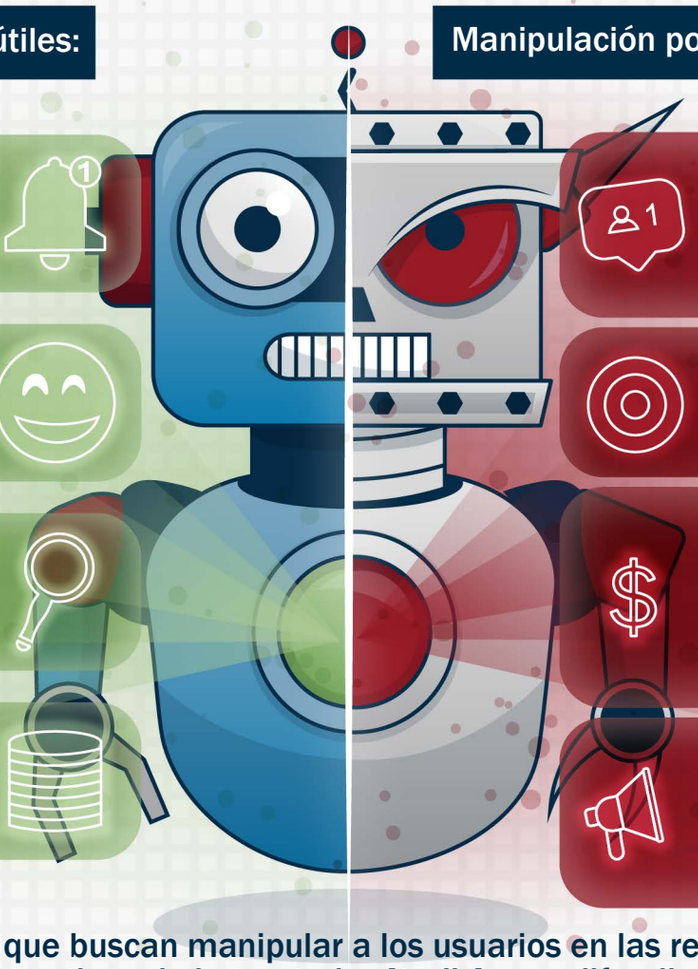
Apoyo por parte de bots útiles:

Notificaciones
Publican actualizaciones automáticamente cuando ocurre un evento de activación`

Entretenimiento
Generan contenido humorístico o noticias agregadas

Búsquedas
Permiten búsquedas de palabras clave y detectan actividades peligrosas

Comercio
Proporcionan atención al cliente o programan publicaciones para marcas



Manipulación por parte de bots nocivos:

Popularidad
Incrementan artificialmente el número de seguidores y comparten publicaciones para aumentar la percepción de influencia

Acoso
Amenazan o arruinan la reputación de cuentas especificas hasta el punto de lograr desactivarlas

Estafa
Phishing de información personal [*Capturan información personal digitalmente de manera fraudulenta*] o promocionan un producto

Operaciones de información
Difunden propaganda para limitar la libertad de expresión y manipular los procesos democráticos

Los actores maliciosos que buscan manipular a los usuarios en las redes sociales a menudo emplean diferentes tipos de bots y troles [*trolls*] para difundir contenido falso:

Los bots **automatizados** funcionan únicamente a través de lenguajes de programación que se ejecutan sin necesidad de gestión humana. Se pueden comprar para ejecutar acciones simples y dar la impresión de influencia.

Los bots **semiautomáticos** permiten al usuario programar un conjunto de parámetros, pero requieren gestión humana, como cuentas falsas. Estos cíborgs [*cyborgs*] son mejores para evadir detección.

Los **troles** [*trolls*] son usuarios humanos, a menudo con identidades ocultas, que buscan crear división en línea. Los agentes criminales pueden emplear bots en combinación con troles [*trolls*].

*Bot es un acortamiento que se refiere a un programa de computadora que actúa como una cuenta automatizada.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés) produjo este gráfico con el fin de resaltar las tácticas utilizadas por las campañas de desinformación que buscan perturbar la vida en los Estados Unidos y la infraestructura crítica que la sostiene. La publicación por parte de CISA de materiales informativos sobre este tema está destinada para conocimiento público y no tiene la intención de restringir, disminuir o denigrar el derecho de cualquier persona a tener, expresar o publicar cualquier opinión o creencia, incluso cuando dichas opiniones o creencias se alinean con las de un gobierno extranjero, se expresan mediante una campaña respaldada por un gobierno extranjero, o disienten de la mayoría

Por favor, tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios - LanguageAccess@cisa.dhs.gov.

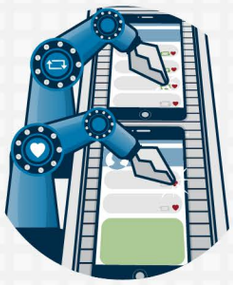
Please note: CISA recognizes that language is continually evolving and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov.

SOCIAL MEDIA BOTS*

Los bots en redes sociales apoyan el comportamiento no auténtico y coordinado de los agentes criminales y amenazan nuestra capacidad para tener importantes debates democráticos. Visite CISA.gov/MDM para obtener más información

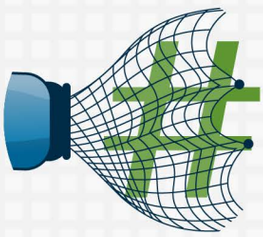
Los bots en redes sociales a menudo forman parte de esfuerzos no auténticos a mayor escala, a través de los cuales las cuentas, tanto administradas por humanos como aquellas automatizadas, trabajan de manera coordinada con el fin engañar al público. Al comprar o configurar sus propios bots, los agentes criminales pueden incrementar sus esfuerzos por difundir información falsa o engañosa, eliminar a la oposición, y elevar sus propias plataformas con el fin de ampliar su capacidad de manipulación.

Saber cómo los bots apoyan actividades no auténticas puede ayudarnos a mitigar sus ataques.



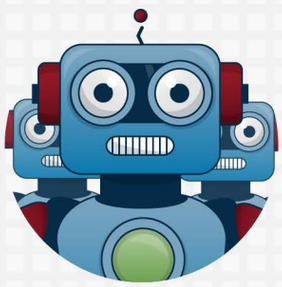
Obtención de clics o de reacción "Me gusta" [*Click/Like Farming*]

Los bots incrementan la popularidad de una cuenta al darle "me gusta" o al publicar de nuevo su contenido. La percepción de influencia en línea puede traducirse en influencia real y distorsionar lo que realmente importa.



Apropiación de etiquetas [*Secuestro de hashtags*]

Los bots atacan a una audiencia aprovechando las etiquetas [*los hashtags*] del grupo (por ejemplo, usando correos basura [*spam*] o enlaces maliciosos), silenciando opiniones opuestas, y desalentando la discusión abierta.



Red de reenvío de publicaciones [*Repost Network*]

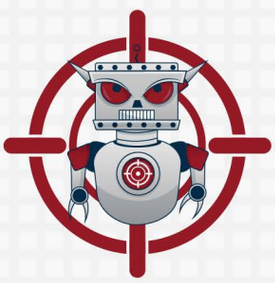
Los bots coordinados (*"botnet"*) publican nuevamente y de manera instantánea el contenido de un bot "principal", inundando las redes sociales con contenido no auténtico que puede influir en la opinión pública y socavar los hechos.

Bots inactivos o bots durmientes [*Sleepers*]

Los bots se despiertan luego de largos períodos de inactividad con el fin lanzar miles de publicaciones o retuits en poco tiempo. El aumento súbito en la atención a un tema puede generar una falsa sensación de urgencia.

Campañas artificiales [Operación de *'Astroturfing'*]

Los bots comparten contenido de manera coordinada, con el fin de dar una falsa impresión de apoyo u oposición popular a un tema de interés público, lo que hace que parezca más importante de lo que es.



Bombardeos o Asaltos [*Raids*]

Los bots se multiplican y sobrecargan cuentas específicas con correos basura [*spam*], acosando al usuario y silenciando las opiniones opuestas.

A medida que las redes sociales se vuelven cada vez más importantes para conectarse entre sí, los ataques de bots ayudan a los agentes criminales a perturbar la democracia, contaminando las conversaciones en línea sobre temas de interés público.

- **Erosionar la confianza en las instituciones** manipulando discusiones orgánicas.
- **Influir en nuestras prioridades** manipulando discusiones orgánicas.
- **Polarizarnos** hacia posiciones más extremas que impiden un diálogo sano.
- **Reprimir la participación** silenciando opiniones contrarias.

*Bot es un acortamiento que se refiere a un programa de computadora que actúa como una cuenta automatizada.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés) produjo este gráfico con el fin de resaltar las tácticas utilizadas por las campañas de desinformación que buscan perturbar la vida en los Estados Unidos y la infraestructura crítica que la sostiene. La publicación por parte de CISA de materiales informativos sobre este tema está destinada para conocimiento público y no tiene la intención de restringir, disminuir o denigrar el derecho de cualquier persona a tener, expresar o publicar cualquier opinión o creencia, incluso cuando dichas opiniones o creencias se alinean con las de un gobierno extranjero, se expresan mediante una campaña respaldada por un gobierno extranjero, o disienten de la mayoría

Por favor, tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios - LanguageAccess@cisa.dhs.gov.

Please note: CISA recognizes that language is continually evolving and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov.

SOCIAL MEDIA BOTS*

Aunque los bots en redes sociales intentan imitar a los usuarios humanos, algunas características pueden indicador un comportamiento no auténtico. Reconocer el comportamiento no auténtico puede aumentar la resiliencia a la manipulación. Visite CISA.gov/MDM para obtener más información.

Cómo detectar un bot

1. Imagen de perfil
Puede ser robado de usuarios reales, generado por IA, una caricatura, a veces detectable mediante la búsqueda inversa de imágenes.

2. Nombre de usuario
Contiene números sospechosos y/o usa mayúsculas de manera inusual.

3. Biografía
Contiene contenido divisivo que atrae a un grupo en particular, pero contiene escasa información personal.

4. Fecha de creación
Cuenta recientemente activada o que solo se activó poco después de un período de inactividad.

5. Cuentas seguidas
La cuenta sigue a una gran cantidad de otras cuentas con el fin generar seguidores y puede ser seguida por una gran cantidad de cuentas casi idénticas (p. ej., seguir para seguir).

6. Red coordinada
Vuelve a publicar con frecuencia desde otras cuentas sospechosas o comparte contenido similar en coordinación con otras cuentas sospechosas.

7. Compartir
Vuelve a publicar la mayoría del contenido de otros usuarios en lugar de crear publicaciones originales, a menudo compartiendo sin expresar una opinión.

8. Contenido viral
Comparte contenido que provoca una respuesta emocional y que puede ser publicado de nuevo fácilmente, tales como memes y GIF; spam hashtags definidos; o utiliza emoticones y puntuación de manera específica.

9. Comportamiento errático
Comparte contenido sobre muchos temas no relacionados entre sí, o cambia de intereses y en comportamiento súbitamente, como al publicar en un nuevo idioma repentinamente.

10. Hiperactivo
Comparte una gran cantidad de contenido, a veces sin parar durante todo el día o con picos de actividad en momentos específicos.

*Bot es un acortamiento que se refiere a un programa de computadora que actúa como una cuenta automatizada.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés) produjo este gráfico con el fin de resaltar las tácticas utilizadas por las campañas de desinformación que buscan perturbar la vida en los Estados Unidos y la infraestructura crítica que la sostiene. La publicación por parte de CISA de materiales informativos sobre este tema está destinada para conocimiento público y no tiene la intención de restringir, disminuir o denigrar el derecho de cualquier persona a tener, expresar o publicar cualquier opinión o creencia, incluso cuando dichas opiniones o creencias se alinean con las de un gobierno extranjero, se expresan mediante una campaña respaldada por un gobierno extranjero, o disienten de la mayoría

Por favor, tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios - LanguageAccess@cisa.dhs.gov.

Please note: CISA recognizes that language is continually evolving and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov.