Managed secure IT | no matter what

¿QUÉ SON LOS BOTNETS Y PORQUÉ SON LA NUEVA AMENAZA DE 2018?

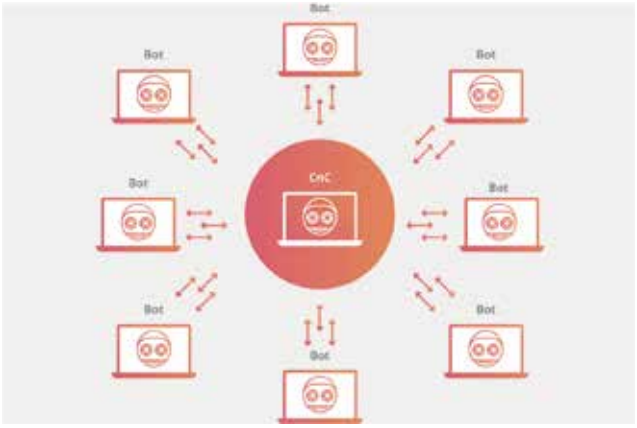
Una red del tipo botnet es una serie de equipos infectados que son controlados por uno o más cibercriminales para actuar de manera remota.

Las botnets se usan para colapsar servicios y redes mediante ataques DDoS y nutrir campañas de Spam. En 2017, se consideró el ascenso de este tipo de redes, como una de las amenazas para la ciberseguridad más peligrosas.

Security

De no protegerse adecuadamente, la red de una compañía o negocio podría convertirse en una botnet sin que los empleados o incluso los CIO's se den cuenta, por lo cual es muy importante saber interpretar las señales que nos indican que nos hemos vuelto parte de una.

Un gran número de estudios indican que en 2018, el uso de las botnets no hará más que crecer, en especial considerando el avance del mercado de los dispositivos de IoT (Internet of Things), que cada vez nos acercan más a convertirnos en víctimas del cibercrimen.

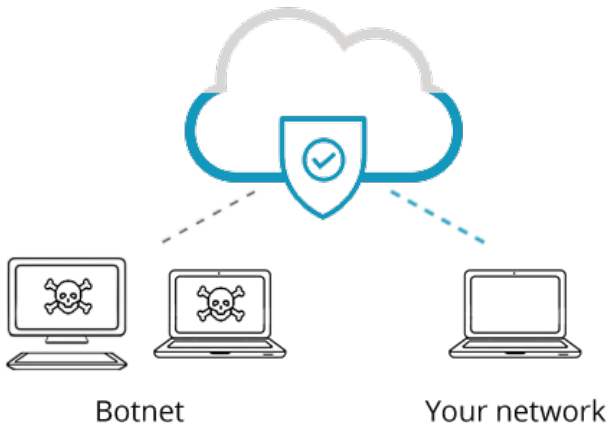


Los equipos que forman parte de una botnet ejecutan comandos enviados por un cibercriminal y pueden llegar a robar información personal, así como infectar su disco duro con códigos maliciosos que podrían infectar a toda una red empresarial.

Las consecuencias de formar parte de una botnet suelen ser gastos millonarios, como el que sucedió con una gran empresa de Estados Unidos que en 2017 tuvo que pagar millones de dólares a un grupo de especialistas en ciberseguridad solo para detener una infección que había afectado a miles de computadoras, portátiles y dispositivos móviles; una baja considerable en el desempeño de los dispositivos infectados y en el peor de los casos, implicaciones legales por haber formado parte de una botnet que se usó para robar información personal de otra organización.

Por esta y más razones, es importante saber cómo evitar convertirse en parte de una botnet, por lo que, entre otras cosas, proponemos:

- Montar una red integral de seguridad que contenga cualquier solicitud de ingreso a una botnet.
- Mantener el cerco de seguridad siempre actualizado.
- Establecer un protocolo de seguridad entre los empleados para evitar infecciones.
- Mantener bien vigilada la entrada y salida de datos a través de los navegadores web.
- Cuidar que las apps en Java se encuentren bien vigiladas.
- Tener un equipo de especialistas en TI que monitoreen toda la red.
- Contar con un plan de acción para evitar el contagio de toda la red en caso de infección.
- Establecer un ciclo constante de respaldos de información para evitar robos.
- Cuidar los dispositivos externos del IoT que se conecten a los equipos de la empresa.
- Migrar las bases de datos y paquetes de apps al cloud para protegerlos.
- Administrar el intercambio de archivos e información en la nube.



Todos estos pasos podrían sonar complejos y, para ser sinceros, son demasiados, pero de no seguir la mayoría, una empresa de cualquier calibre y giro podría convertirse en parte del arsenal de los cibercriminales, aun contra su voluntad.

Los expertos coinciden en que los botnets serán una de las amenazas más graves de 2018 y que su proliferación no se detendrá pronto, así que existen dos maneras de seguir estas recomendaciones de seguridad: contar con un nutrido equipo de especialistas en TI que trabajen en una oficina nueve u ocho horas seguidas de lunes a viernes o, pagando extra, 24 horas de lunes a domingo; o la otra alternativa, buscar la asesoría de un grupo de expertos en seguridad que hablen tu idioma y construyan un plan de seguridad a la medida de tus necesidades.

Además de proteger tu información e informarte de cómo cuidarla, este equipo de expertos podrá mantener un cerco de seguridad desde el blindaje de la nube y de manera remota, atendiendo cualquier eventualidad y previniendo el avance de cualquier amenaza a todas horas, sin importar el día de la semana.

Síguenos en nuestras redes sociales:

MexisMX

Servicios Administrados Mexis, S.A. de C.V.

Mexis TI

Servicios Administrados Mexis, S.A. de C.V.