NOTA DE PRENSA
04 / 01 / 2021

El 54% de los ataques lanzados durante el tercer trimestre fueron de tipo phishing

> En segunda posición, se encuentran los ataques adware, es decir, aquellos relacionados con la publicidad que invade a los usuarios cuando navegan por Internet

Allot, compañía dedicada a la protección de redes y de usuarios de cualquier tipo de ataques, incluyendo malware, ransomware, phishing y cryptojacking, ha publicado su informe trimestral *'Cyber Threat Report'*, cuyos datos se basan en ataques de tipo malware, entre otros, que han sido detectados y bloqueados por la herramienta de Allot NetworkSecure durante el tercer trimestre del año 2020 en Europa.

El informe refleja cómo los ciberdelincuentes han intensificado sus ataques, sobre todo dirigidos a las personas cuando éstas son más vulnerables a estafas y otros delitos, en un momento en el que las empresas cuentan con muchos de sus empleados trabajando en remoto a causa de la pandemia. Además, los datos muestran una evolución similar de los ataques con la curva de contagios por el virus en Europa. Por ejemplo, en el tercer trimestre Allot bloqueó alrededor de 750 millones de URLs maliciosas en todo el continente, de las cuales un 32% se detectaron en julio, un 30% en agosto y un 36% en septiembre, cuando el pico de contagios estaba creciendo.

"Somos más vulnerables a sufrir ataques cuando estamos en casa porque nos relajamos inconscientemente ya que creemos que en nuestro hogar estamos a salvo y contamos con los mismos medios de acceso que teníamos en la oficina. Sin embargo, en muchas ocasiones, esto no es así", explica Carmen Vega, Sales Director para Iberia de Allot.

Phishing y adware, los ciberataques más utilizados

El phishing sigue siendo el ataque más predominante en Europa, con una cifra que llega al 54% de media de los bloqueos ocurridos durante estos tres meses, sólo un 1% por debajo del trimestre

anterior. Aunque esta técnica es una de las más utilizadas por los ciberdelincuentes, la crisis del coronavirus ha incentivado su uso y la Covid-19 se ha convertido en el principal gancho, aprovechando el miedo de la población –tanta es la vinculación que existe con la curva de contagios del virus que, a finales de septiembre, el porcentaje de ataques de tipo phishing que detectó y bloqueó Allot NetworkSecure superaba el 58%–. A esto se suma que los sitios web falsos son prácticamente imposibles de detectar por el ojo humano. "Los ciberdelincuentes continúan utilizando este tipo de ataques porque tienen éxito. Es muy fácil caer en las páginas webs porque están muy bien hechas, por eso es importante tener mucha precaución y saber bien dónde hacemos clic", comenta Vega.

Caer en un ataque phishing conlleva graves daños como la pérdida económica o el robo de datos personales y de credenciales de cuentas comprometidas.

En segunda posición, se encuentran los ataques de adware, es decir, aquellos relacionados con la publicidad que invade a los usuarios cuando están conectados a Internet. Allot estima que alrededor de un 30% de las amenazas bloqueadas durante el tercer trimestre fueron de este tipo. El adware, además de ser una molestia para los usuarios ya que provoca una sensación de pérdida de privacidad, puede causar graves daños. Al igual que otro tipo de malware, este ciberataque puede infectar los terminales de los usuarios al redirigirlos a páginas con contenido malicioso. "Un adware puede resultarnos atractivo y más si nos encontramos en un momento relajado. Sin pensar, pinchamos en el anuncio e inmediatamente nos envía a una web de phishing, en la cual ya estamos atrapados", afirma la directiva.

En las siguientes posiciones y a mucha distancia del phishing y el adware, Allot sitúa a los ataques relacionados con los bitcoins y el contenido para adultos, con unos resultados que oscilan entre el 1 y el 10% de las amenazas bloqueadas durante la época estival.

"En un momento en el que las empresas están experimentando fuertes picos de teletrabajo a causa de la pandemia del coronavirus, los ciberdelincuentes han intensificado sus ataques, dirigiéndose a las personas cuando son más vulnerables a estafas y otros delitos", señala Barry Spielman, Product Marketing Director de Allot Secure.

Allot recomienda no relajarse durante el teletrabajo y tener mucha precaución cuando se hace clic en una URL que proviene de un email o de un anuncio atractivo. Siempre es mejor buscar el contenido y abrirlo desde el propio navegador.

Para más información, puede acceder al informe completo aquí.

Contacto de prensa:

JAVIER MODUBAR ALVAREZ
info@ingecom.net
944395678
http://www.ingecom.net