

CIBERSEGURIDAD Y CONFIANZA EN LOS HOGARES ESPAÑOLES

El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) de Red.es ha hecho público el “Estudio sobre la Ciberseguridad y Confianza de los hogares españoles”, realizado a partir del panel *on line* compuesto por aquellos hogares con conexión a Internet repartidos por todo el territorio nacional.

Según los datos del estudio:

Internet sigue siendo considerado como cada día más seguro (44,1%), los equipos se consideran razonablemente protegidos (68,5%) y se relaja el hábito de realización de copias de seguridad (55,9%,)

Una gran parte del *software* malicioso resulta novedoso e innovador, con lo que puede eludir las detecciones de las soluciones antivirus basadas en firmas (hasta un 47% del *malware* detectado en el segundo trimestre de 2017), o se va transformando continuamente para adaptarse (como el *adware* ‘Stantinko’, que ha logrado pasar desapercibido durante 5 años). Ello pone de manifiesto la importancia de mantener actualizados los antivirus basados tanto en el motor como en las firmas.

El uso real de soluciones antivirus por parte de los internautas españoles es más relajado que el uso declarado. El 61,7% de los usuarios de ordenadores y el 28,1% de dispositivos Android, no se percatan de las infecciones existentes en sus equipos, lo que podría estar causando una falsa sensación de seguridad. 7 de cada 10 de estos equipos se encuentran en riesgo alto debido a la tipología de *malware*.

Los usuarios analizan todos los ficheros descargados desde redes P2P (59,6%) descarga directa (46,6%), e instala aplicaciones Android principalmente desde repositorios oficiales (92,8%) para evitar incidencias de seguridad.

Uno de los objetivos del *malware* es la creación de *botnets*, que son grupos de ordenadores y dispositivos comprometidos -llamados *bots* o *zombies*- controlados remotamente para realizar ataques DDoS, hacer *spam*, etc. En este sentido España es el quinto país europeo con más equipos formando parte de estas redes, destacando la ciudad de Madrid en número de los mismos. Ello pone de manifiesto la importancia de cambiar las contraseñas de acceso a servicios online con cierta periodicidad (actualmente sólo el 33,2% de los usuarios españoles lo hace cuando tiene constancia de una incidencia de seguridad).

La principal motivación que mueve a los desarrolladores de *malware* es el beneficio económico que sus códigos les pueden reportar (*adware*, troyanos bancarios, *ransomware*, etc.). El hecho de que durante los últimos meses de 2017 se haya experimentado un gran crecimiento en el valor del Bitcoin, ha propiciado que las criptomonedas se sitúen en el punto de mira de éstos, ya que podrían resultar en una importante fuente de ingresos. Así, se han divisado muestras que, con el objetivo de robar criptodivisas y sus *wallets* (monederos digitales), crear *botnets* (de servidores, ordenadores personales y dispositivos móviles, etc.) para utilizar la capacidad de procesamiento en pos de la minería, insertar *script* en sitios web para aprovechar los recursos de las máquinas usadas por los visitantes, etc.