El Periódico de Catalunya
España
10/07/17
Prensa: Diaria
Tirada: 55.842 Ejemplares
Difusión: 45.744 Ejemplares
Cód: 111638214
Página: 30
Sección: SOCIEDAD Valor: 20.235,00 € Área (cm2): 975,1 Ocupación: 80,62 % Documento: 1/2 Autor: CARMEN JANÉ I BARCELONA Núm. Lectores: 508000

Vigilancia en la red

Los policías del ciberespacio

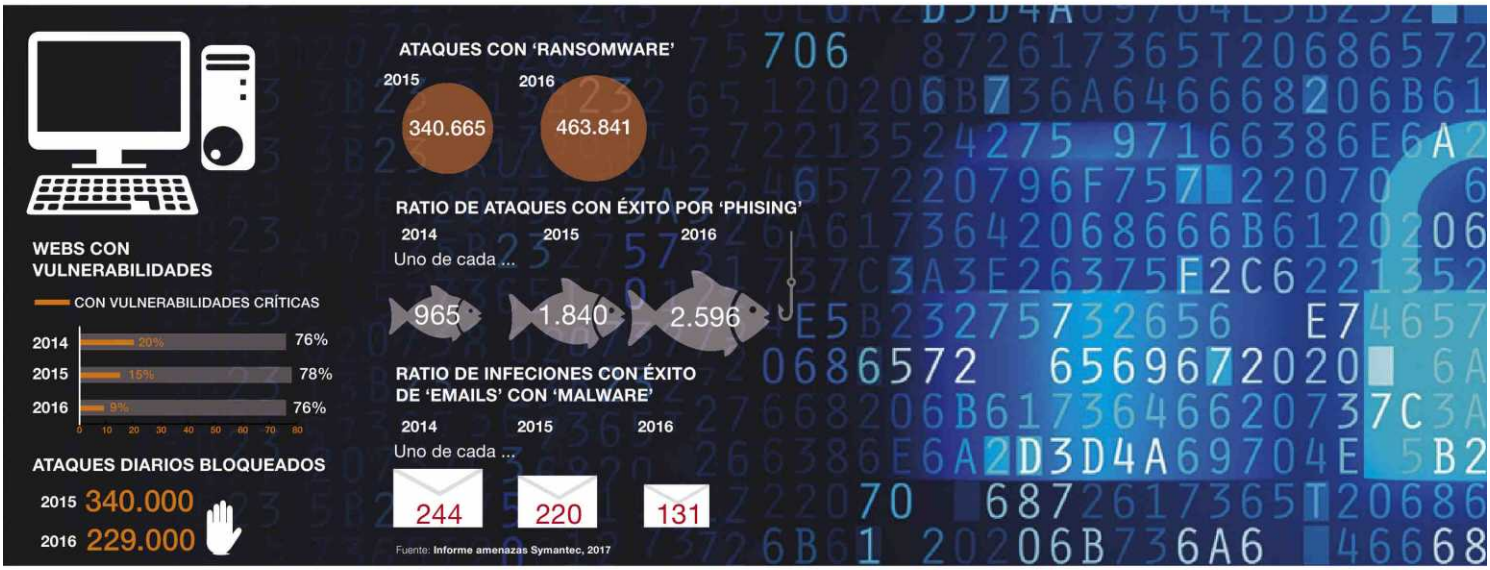
Un total de 380 equipos de todo el mundo se coordinan como centros de respuesta ante un ataque informático

CARMEN JANÉ
BARCELONA

Si las redes informáticas son el nuevo canal por el que se mueve la información y la economía mundial, también tienen sus vigilantes que se encargan de que todo el mundo pueda navegar y hacer transacciones sin problemas desde hace casi 30 años. Son los Equipos de Respuesta ante Incidentes de Seguridad Informática (en inglés CSIRT, como se les conoce en Europa, o CERT para los estadounidenses), creados por gobiernos, universidades y empresas para intentar mantener el tráfico de las redes limpio de virus, ataques de denegación de servicio, *malware* o *spam* masivo. Y los últimos virus masivos, como el Wannacry o el Petya/NotPetya los han puesto a prueba. Los CERT son, por lo general, lugares modestos. En el esCERT-UPC, de la Universitat Politècnica de Catalunya (UPC), el más veterano de España, una espera hallar un local lleno de pantallas que muestren en directo el flujo de ataques informáticos del mundo sobre un mapamundi en la más pura estética *Juegos de guerra*. Pero lo que hay es un sótano con ordenadores como los de cualquier empresa, lleno de carteles con bromas informáticas y con siete personas trabajando.

AUDITORÍAS // «Hay quien debe controlar más información, avisos, de muchas fuentes... y necesitan las pantallas», afirma el catedrático Manel Medina, fundador y director del esCERT-UPC desde 1994. Otros CERT, como el de los bancos, son en apariencia más sofisticados. Porque, en informática, la realidad es lo que desde fuera no se ve. Y en este sótano se hacen auditorías de seguridad (se intentan ver los puntos débiles de los sistemas informáticos de otros), análisis forenses (qué ha pasado y por qué) o ayuda ante incidentes de administraciones locales, universidades y pymes. Y siempre con una oreja virtual puesta en los foros de seguridad y lo que se cuece en el mundillo *underground*, según Medina.

Hay más de 380 CERT en todo el mundo, según la red FIRST, en la que se autocoordinan a nivel mundial e intercambian información centros creados por gobiernos (hasta Bután tiene el suyo), empresas como Amazon, Apple, Caixabank, BBVA, Google, Airbus, Bank of America, Paypal, Telefónica..., que se autofinancian, y organismos de investigación, que reciben fondos de gobiernos. Solo la Unión Europea destina más de 10,8 millones de euros a reforzar la red CSIRT, que se coordina también por el foro Abuses a nivel español, en el que participan los proveedores de servicios de internet. En España, el CERT más importante es el CNN-CERT, que depende del Centro Nacional del Inteligencia y emite los



Negocio antes que seguridad

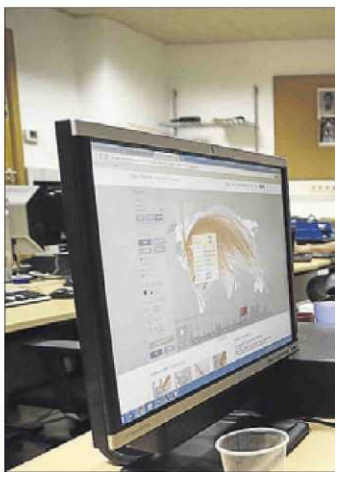
Las actualizaciones de programas a veces se posponen para no afectar a la actividad de la empresa ≡ **Los informáticos** de sistemas corporativos prefieren limitar el permiso a los usuarios

C. J.
BARCELONA

Para muchas empresas, la seguridad de las redes donde hacen la mayor parte de sus negocios no son lo más importante y hay actualizaciones de programas que se posponen solo para que no les afecten. La queja parte del esCERT-UPC pero es compartida por muchos otros administradores de sistemas. Una de las grandes evidencias tras los recientes ataques del Wannacry y el Petya/NotPetya ha sido que muchas empresas no habían actualizado sus sistemas operativos. **«Puede ser porque usan programas propios que no les funcionarían en sistemas más nuevos o porque les supondría parar sus ordenadores durante algunas horas»,** afirma Manel Rodero, del esCERT-UPC.

Los daños, sin embargo, pueden ser más duros. Reckitt Benckiser, dueño de marcas como Durex, Harpic o Nurofen, calculó el pasado jueves, en la presentación de resultados de sus empresas, que el virus Petya les ha costado 133 millones de euros, un punto porcentual en la facturación global de la compañía. El virus, explicó, impidió enviar y facturar pedidos y afectó a varios centros de producción. También la naviera danesa Maersk y el grupo de alimentación Mondelez tuvieron que suspender operaciones aunque no han hecho públicas las pérdidas.

Las políticas de permitir a los empleados usar sus propios dispositivos en parte para ahorrar gastos pueden empeorar los efectos de un ataque. Son equipos portátiles que no se conectan habitualmente y por tanto no reciben las actualizaciones previstas por el departamento de informática, o solo las relativas a equipos domésticos. Es el caso del típico



El Periódico de Catalunya
España
10/07/17
Prensa: Diaria
Tirada: 55.842 Ejemplares
Difusión: 45.744 Ejemplares
Cod: 111638214
Página: 31
Sección: SOCIEDAD Valor: 21.210,00 € Área (cm2): 1022,1 Ocupación: 84,5 % Documento: 2/2 Autor: CARMEN JANÉ I BARCELONA Núm. Lectores: 508000

Gobiernos, universidades y empresas **mantienen las patrullas** que vigilan las agresiones de virus en internet

niveles de alerta en ciberseguridad. En Catalunya, Cesicat ejerce como CERT de la Administración catalana, entidades locales y empresas.

Cuando los incidentes de seguridad exigen persecución de la delincuencia, el tema deriva al European Cybercrime Center (EC3), en el que participa Europol, la organización de las policías europeas. Igual que a escala nacional, porque los vigilantes de la red denuncian pero no detienen. Y luego está ENISA, la agencia europea de seguridad informática.

La cooperación lleva a los CERT a compartir información, que fluye a través de una lista de correo restringida y con mensajes encriptados e informes ultraconfidenciales. «Hay cuatro niveles de confidencialidad, desde el de divulgación general, al que solo puede leer quien puede ejecutar órdenes concretas, el *solo para sus ojos*. Porque hay datos que no se pueden difundir hasta que se toman medidas porque podría desactivar toda la operación contra un ataque», dice Antonio Rodríguez, responsable de ciberseguridad del esCERT-UPC.

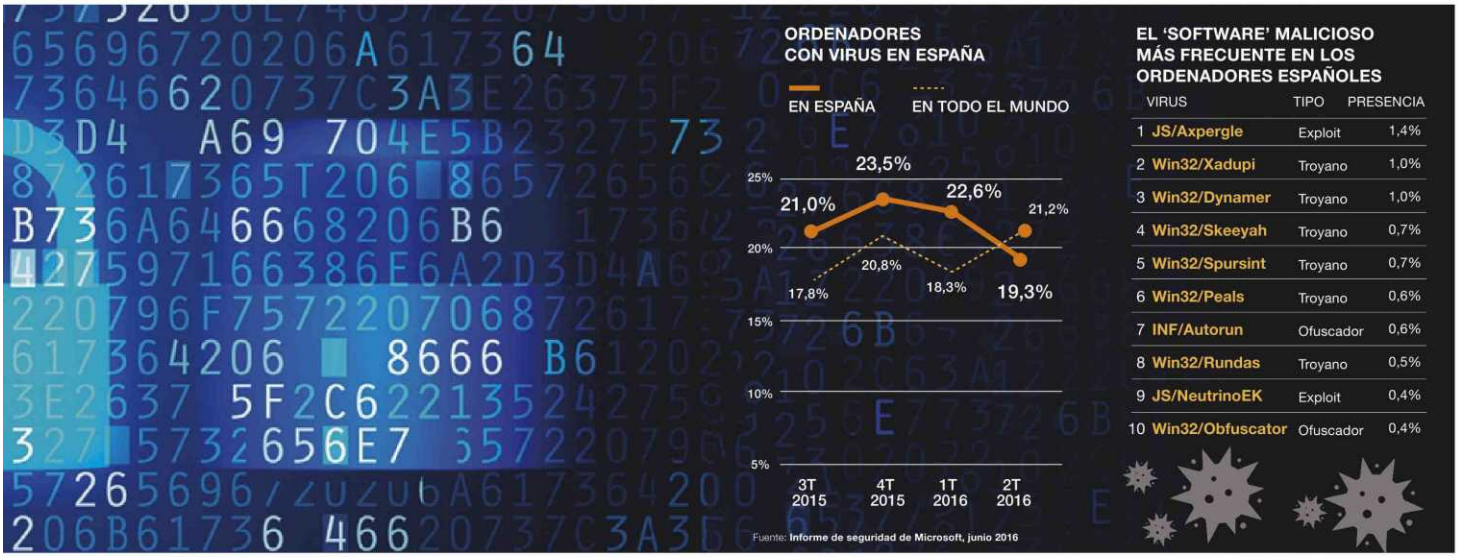
Ante un ataque como el del *ransomware* Wannacry, que aprovechaba un fallo de seguridad en Windows que Microsoft ya había parcheado pero que muchos administradores de sistemas no habían actualizado, tuvieron que hacer trabajos extra. Su día a día incluye lidiar con intentos de intrusión, ataques, virus, correos con archivos fraudulentos o *spam*. Y avisar cuando hay algo anómalo. «Las alertas de los antivirus ya no saltan mucho, ahora son cosas más complejas», señala Rodríguez.

«Puede ser porque alguien quiera copiar artículos protegidos por *copyright*, intentos de entrada en servidores no autorizados, usar las máquinas para alojar porno infantil, lo que quieran... A veces te enteras porque te vienen los Mossos. Una red universitaria, como tiene mucha capacidad, es un objetivo preferente

Su día a día incluye lidiar **con intentos de intrusión,** 'spam' o correos con archivos fraudulentos

para enviar desde aquí un ataque a otros», señala Manel Rodero, técnico de esCERT-UPC. «Cada vez más gente se conecta desde otros lugares a los ordenadores de la UPC, así que eso también hay que asegurarlo», añade Antonia Gómez, responsable del área de sistemas de inLab.

ANALISTA DE DATOS // Entonces hay que recopilar información sobre las entradas a las máquinas, las sondas en puntos delicados de la red, cruzar datos y analizarlos. Y para eso es muy valioso tener automatizados los sistemas de detección. «A veces la información sobre lo que está pasando no la tienes en directo, sino que hay que cotejar herramientas para hacerte una idea. Las hay comerciales y propias, propietarias y sofware libre», señala Gómez. «La de analista de datos es una profesión de futuro, porque hay que ser capaz de interpretar qué ocurre antes de tomar una decisión», afirma Rodero. ≡



EL 'SOFTWARE' MALICIOSO MÁS FRECUENTE EN LOS ORDENADORES ESPAÑOLES

	VIRUS	TIPO	PRESENCIA
1	JS/Axpergle	Exploit	1,4%
2	Win32/Xadupi	Troyano	1,0%
3	Win32/Dynamer	Troyano	1,0%
4	Win32/Skeeyah	Troyano	0,7%
5	Win32/Spursint	Troyano	0,7%
6	Win32/Peals	Troyano	0,6%
7	INF/Autorun	Ofuscador	0,6%
8	Win32/Rundas	Troyano	0,5%
9	JS/NeutrinoEK	Exploit	0,4%
10	Win32/Obfuscator	Ofuscador	0,4%

JULIO CARBÓ

Responsables del centro de respuesta a ataques informáticos CERT de la UPC.

ordenador portátil de un ejecutivo o un comercial, por ejemplo. **«Hay que hacer mucha política de prevención y concienciación de los usuarios, y que tengan claro que no pueden abrir cualquier archivo que se les envía»,** explica Antonia Gómez.

Recomendación

Pero no siempre son archivos en correos los que inician un ataque de *ransomware*. Circuló el rumor con Wannacry pero se descartó y tampoco parece haber sido la vía para Petya/NotPetya, el último virus que se ha difundido globalmente.

Una de las recomendaciones del esCERT-UPC, y de algunas compañías de antivirus, como Sophos, es precisamente limitar los privilegios de los usuarios, es decir que para instalar un programa sea necesaria una clave. **«A los usuarios les irrita mucho, pero evita muchos disgustos. No puede ser que estés trabajando siempre en un ordenador con acceso a todo el sistema operativo. Las buenas prácticas son trabajar con una cuenta para las tareas habituales y cuando hay que instalar programas o actualizaciones, usar otra. Solo así se evitan disgustos. Por eso también en parte se dice que Linux o Unix son más seguros, porque en Linux o en Unix no trabajas desde el administrador»,** señala Antonio Rodríguez, jefe de ciberseguridad del esCERT-UPC.

El virus Petya ha costado 133 millones de euros a la firma Reckitt Benckiser

Los expertos son partidarios de que para instalar un programa se necesite una clave

Otro punto conflictivo es el acceso permanente a servicios de copia remota como Dropbox. **«Si te llega un *ransomware*, el programa comenzará a cifrar carpetas, tanto del disco duro como de la copia virtual, y lo perderás todo»,** avisan. ≡