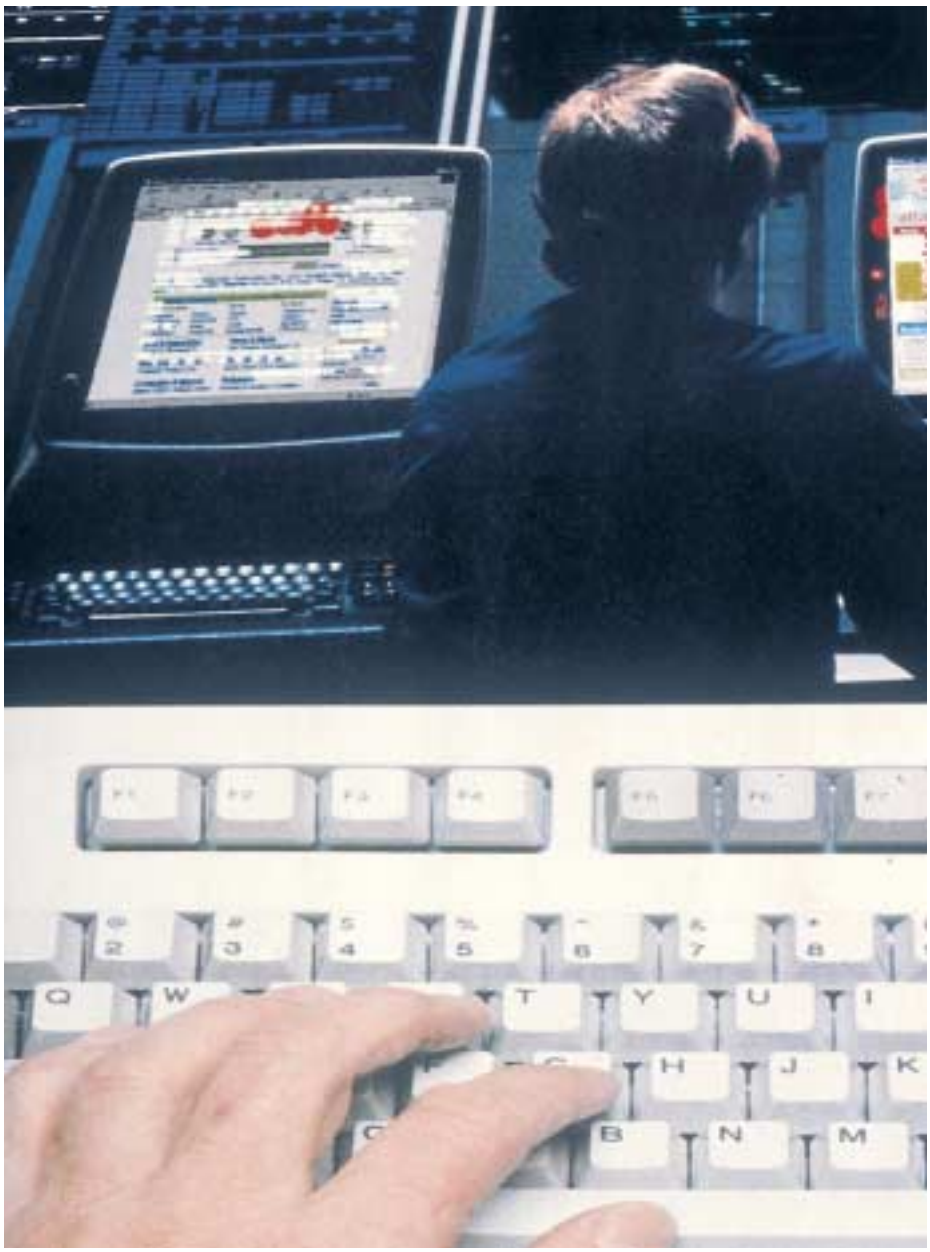
Un informe sobre amenazas a la seguridad en Internet de Symantec presentado el pasado mes de abril desvela que los ataques evolucionan a medida que los atacantes buscan información de las empresas y los usuarios. La actividad maliciosa en la Red siguió creciendo a un ritmo récord el año pasado.

La actividad maliciosa en la Red se desboca

De acuerdo con el Informe de Symantec sobre «Amenazas a la Seguridad en Internet Volumen XIV», la compañía detectó más de 1,6 millones de nuevas firmas de código malicioso en 2008. Esto equivale a más del 60 por ciento del total de firmas de códigos maliciosos detectadas por Symantec a lo largo del tiempo, y demuestra su gran proliferación y aumento de volumen. Gracias a esta capacidad de descubrir amenazas, durante 2008 Symantec consiguió bloquear un promedio mensual de 245 millones de intentos de ataque de códigos maliciosos en todo el mundo.

El Informe sobre Amenazas a la Seguridad en Internet ofrece una visión mundial del estado de la seguridad en la Red derivado de los datos recolectados por millones de sensores de Internet, investigaciones de primera mano y una activa monitorización de las comunicaciones de los hackers. El periodo de observación comprendido por el ISTR XIV abarca de enero a diciembre de 2008.

El informe muestra que la navegación por Internet se mantuvo como la principal fuente de nuevas infecciones en 2008, y que los atacantes confían cada vez más en herramientas de código malicioso hechas a medida para desarrollar y distribuir sus amenazas. Además, el 90 por ciento de todas las amenazas detectadas por Symantec durante el periodo de estudio estaban destinadas a robar informa-



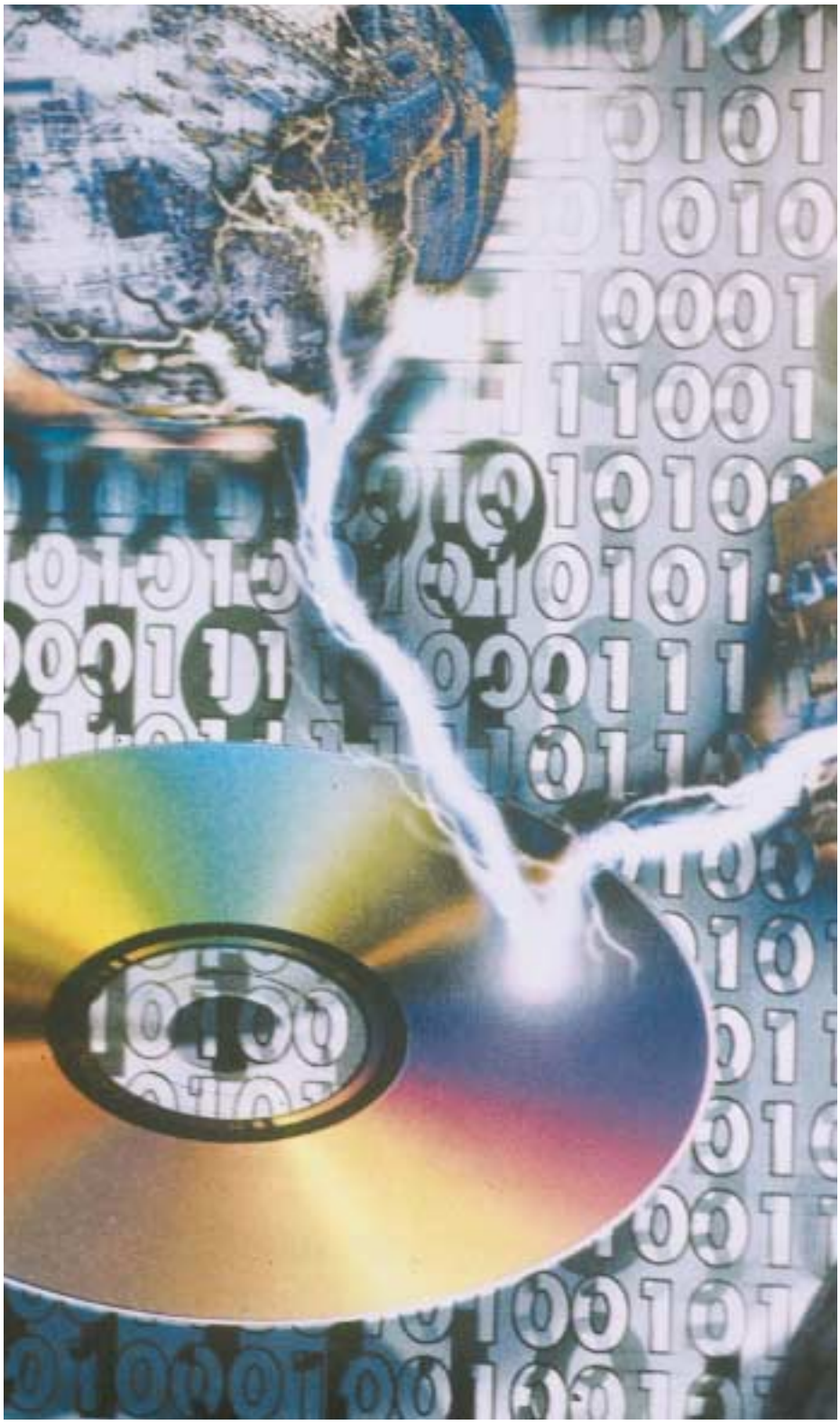
ción confidencial. Las amenazas con capacidad de registrar las pulsaciones del teclado, que pueden ser utilizadas para robar información como los datos de acceso a cuentas de banca electrónica, representaron el 76 por ciento de las amenazas a la información confidencial, lo que supone un ligero crecimiento sobre el 72 por ciento registrado en 2007.

Basado en la información del Informe de Symantec sobre la Economía Sumergida, Symantec concluye que continúa existiendo una economía sumergida bien organizada y especializada en la venta de datos confidenciales robados, particularmente los relacionados con tarjetas de crédito y credenciales de cuentas bancarias. Esta economía sumergida está floreciendo; así que mientras que los precios de los bienes en el mercado legítimo están cayendo, los precios en la economía sumergida han permanecido estables de 2007 al 2008.

«Mientras los códigos maliciosos continúan creciendo a un ritmo record, también observamos que los atacantes han cambiado su modelo de operar de una distribución masiva de unas cuantas amenazas a la micro distribución de millones de amenazas distintas», explica Steve Trilling, vicepresidente de Symantec Security Technology and Response. «Los cibercriminales se están lucrando con la creación y distribución personalizada de amenazas que roban información confidencial, particularmente credenciales de cuentas de banco y datos de tarjetas de crédito. Así que mientras la economía regular sufre, la economía sumergida se mantiene constante».

El informe también destaca la capacidad de los autores del malware para evadir los intentos de detener sus actividades. Como ejemplo, el cierre de dos sitios que hospedaban botnets (redes bot) en Estados Unidos contribuyó a un descenso significativo en la actividad de botnets durante septiembre y noviembre de 2008; sin embargo, los operadores de estas redes encontraron alojamientos Web alternativos y las infecciones de bots rápidamente recuperaron los niveles que tenían antes del cierre de éstos.

Las plataformas de aplicaciones Web fueron recursos comunes de vulnerabilidades durante el periodo de estudio. Estos productos de software pre-construido son



diseñados para simplificar el desarrollo de nuevos sitios Web y son muy populares en Internet. Muchas de esas plataformas no fueron diseñadas pensando en la seguridad, y por eso tienen numerosos defectos que las hacen vulnerables ante los ataques. De todas las vulnerabilidades identificadas en 2008, el 63 por ciento (394) habían sido solventadas en el momento en el que se redactaba este informe. El estudio de Symantec también encontró que los ataques basados en Web fueron originados desde países alrededor del mundo, y la mayoría se originaron desde Estados Unidos (38 por ciento), seguido de China (13 por ciento) y Ucrania (12 por ciento). Seis de los 10 principales países con más ataques basados en Web están en EMEA (Europa, África y Medio Oriente) y supusieron el 45 por ciento del total mundial de ataques basados en Web, más que ninguna otra región.

2008 Rank	2007 Rank	Country	2008 Percentage	2007 Percentage	Malicious Code Rank	Spam Zombies Rank	Phising Websites Host Rank	Bot Rank	Attack Origin Rank
1	1	Germany	14%	18%	6	1	1	2	2
2	2	United Kingdom	11%	11%	1	7	2	6	1
3	4	Spain	9%	8%	4	5	7	1	4
4	5	Italy	8%	8%	5	3	8	3	5
5	3	France	7%	9%	2	8	5	7	3
6	6	Poland	6%	6%	12	6	4	4	8
7	7	Turkey	6%	4%	7	2	13	5	6
8	8	Russia	6%	4%	9	4	3	10	7
9	9	Netherlands	3%	3%	8	20	6	15	10
10	10	Israel	3%	3%	23	9	9	9	11

Table 1. Malicious activity by country, EMEA.
Source: Symantec Corporation

El informe también muestra que el phishing ha seguido creciendo. En 2008, Symantec detecto 55,389 sitios de alojamiento de phishing, un 66 por ciento más que en 2007, cuando Symantec descubrió 33,428. Los servicios financieros estuvieron presentes en 76 por ciento de los señuelos de phishing en 2008, creciendo desde el 52 por ciento del pasado año.

Finalmente, el ISTR también concluye que el volumen de spam ha seguido aumentando. En el último año, Symantec ha observado un incremento del 192 por ciento en el spam detectado en Internet, de 119,6 mil millones de mensajes en 2007 a 249,6 mil millones en 2008. Cabe mencionar que, en 2008, las redes bot fueron responsables de la distribución de aproximadamente el 90 por ciento del total de todo el spam distribuido por correo electrónico.

HALLAZGOS ADICIONALES

— De acuerdo con datos de Symantec, en 2008, el crecimiento de la actividad de códigos maliciosos fue mayor en EMEA (Europa, Medio Oriente y África).
— En 2008, Symantec observo un promedio de más de 75,000 equipos activos infectados por bots, un 31 por ciento de incremento comparado con 2007.
— A finales de 2008, más de un millón de ordenadores personales fueron infectados por el gusano Downadup (también conocido como Conficker); que era capaz de expandirse rápidamente a lo largo de Internet gracias a un gran número de avanzados mecanismos de propagación. El número de infecciones a nivel mundial de Downadup/Conficker creció hasta llegar a más de tres millones de sistemas infectados durante el primer trimestre del 2009.

ESPAÑA EN EL MUNDO

Actividad maliciosa

— En el ranking a nivel mundial de Actividad Maliciosa registrada por cada país durante 2008, España conserva la 6ª posición que obtuvo en el ISTR anterior, con el 4% de la actividad generada en todo el mundo.
— Tal y como se observa en el gráfico anterior, España obtuvo las siguientes posiciones a nivel mundial:
  - Ranking de Códigos Maliciosos ..... 10ª posición
  - Ranking de Zombies para Spam..... 8ª posición
  - Ranking de Hosts de Sitios Web para Phishing ..... 13ª posición
  - Ranking de Actividad Bot ..... 3ª posición
  - Ranking Países Origen de Ataques ..... 6ª posición
— Dentro de la categoría de Actividad Bot, la 3ª posición que ocupa España la obtuvo con un 8% del total de ordenadores infectados con bots en todo el mundo, por encima de países como Alemania, Italia o Rusia.

ESPAÑA EN LA REGIÓN EMEA

Actividad maliciosa

— En el ranking EMEA de Actividad Maliciosa en general registrada durante 2008, España fue el número 3 con un 9%, con lo que subió una posición con respecto al año pasado.
— En la categoría de Actividad Bot, España desplazó a Alemania y obtuvo la 1ª posición con 15% del total, escalando desde la 2ª plaza obtenida el año pasado.
— Asimismo, en comparación con el año anterior, en 2008 España subió posiciones en todas las categorías sobre Actividad Maliciosa (excepto en País Origen de Ataques, en la cual se mantuvo en el 4º puesto). Tal y como se observa en el gráfico, España obtuvo las siguientes posiciones:
  - Ranking de Códigos Maliciosos .....4ª posición
  - Ranking de Zombies para Spam.....5ª posición
  - Ranking de Hosts de Sitios Web para Phishing .....7ª posición
  - Ranking de Actividad Bot .....1ª posición
  - Ranking Países Origen de Ataques .....4ª posición
— En el volumen anterior del ISTR, se especuló que la actividad bot en España seguiría una tendencia similar a la observada previamente en el Reino Unido; dicha tendencia sugería que el porcentaje de ordenadores infectados

por bots incrementaría a medida que aumentase la penetración de la banda ancha y entonces, eventualmente se estabilizaría mientras las infraestructuras para la banda ancha quedasen establecidas. La tendencia se produce a medida que los usuarios y los proveedores de servicios de Internet (ISPs) adquieren una mayor concienciación sobre la seguridad informática y se convierten más expertos a la hora de implantar medidas de protección para evitar las infecciones. Dicha tendencia parece ser cierta en el caso de España ya que, con un crecimiento de la banda ancha significativamente más lento durante 2008, el comportamiento de la actividad bot reflejó un resultado correlativo, manteniendo el mismo porcentaje que en 2007.

Códigos maliciosos

— Tal y como se muestra en el gráfico, España está incluida en 2 categorías dentro del apartado de países con infecciones potenciales por Códigos Maliciosos en la región EMEA.
— En la categoría de Back Doors (Puertas Traseras), España está en 2º lugar, por detrás del Reino Unido. El año pasado, España estaba en 5ª posición, lo cual es un salto significativo con el que desplazó a Alemania a la 4ª plaza.
— La segunda categoría en la que encontramos a España es la de Gusanos, ocupando la 3ª posición, por detrás del Reino Unido y Arabia Saudita.
— Asimismo, dentro del top 10 de Códigos Maliciosos, el gusano denominado SillyFDC está en la 4ª posición, con España como el país que más reportó la actividad entre sus internautas.

Phishing & Spam

— En el ranking sobre países que albergan sitios web para Phishing, España conserva la 9ª posición en 2008, al igual que el año pasado, con 5% del total de la región EMEA.
— Y finalmente, dentro de los países origen de Spam, en 2008 España descendió 2 posiciones con respecto al año anterior, ocupando la 8ª con un 5% del total de la zona EMEA.

	Top Countries			
Rank	Back Doors	Trojans	Viruses	Worms
1	United Kingdom	United Kingdom	Egypt	Saudi Arabia
2	Spain	France	Turkey	United Kingdom
3	France	Germany	United Kingdom	Spain

Table 7. Geolocation by type of malicious code, EMEA.
Source: Symantec

2008 EMEA Rank	2007 EMEA Rank	2008 Global Rank	Country	2008 EMEA Percentage	2007 EMEA Percentage
1	3	2	Russia	13%	10%
2	8	3	Turkey	12%	4%
3	1	6	United Kingdom	7%	15%
4	4	7	Germany	6%	9%
5	5	8	Italy	6%	6%
6	2	9	Poland	6%	10%
7	111	10	Burundi	5%	<1%
8	6	11	Spain	5%	6%
9	7	14	France	4%	6%
10	20	20	Romania	3%	1%

Table 12. Spam country of origin, EMEA.
Source: Symantec