

## IBM X-Force descubre que el número de datos filtrados se redujo en 2017 mientras cibercriminales se enfocaban en el ransomware

Los errores humanos son responsables de dos tercios de los registros comprometidos, incluido el aumento histórico del 424% en la infraestructura de nube mal configurada.

**CAMBRIDGE - 04 abr 2018:** IBM Security anunció hoy los resultados de su informe "2018 IBM X-Force Threat Intelligence Index", en donde se muestra que la cantidad de registros infringidos cayó casi un 25% en 2017 a medida que los cibercriminales cambiaron el enfoque en el lanzamiento de ransomware y ataques destructivos que buscaban retener o destruir información a menos que la víctima pagara algún rescate.

El año pasado, más de 2.9 mil millones de registros fueron comprometidos reduciendo los 4 mil millones divulgados en 2016. Si bien el número de registros infringidos aún es significativo, el ransomware reinó en 2017 con ataques como **WannaCry**, **NotPetya** y **Bad Rabbit**, que causaron caos en todas las industrias sin registros comprometidos reportados.

Otros hallazgos clave incluyen:

- Un salto histórico del 424% en infracciones relacionadas con la infraestructura de nube mal configurada, en gran parte debido a errores humanos.
- Por segundo año consecutivo, la industria de servicios financieros se posicionó de nuevo como la industria que sufrió la mayor cantidad de ataques en su contra, representando el 27% de los ataques en todas las industrias.

El IBM X-Force Threat Intelligence Index se compone de información y observaciones de datos analizados a través de cientos de millones de endpoints y servidores protegidos en casi 100 países. IBM X-Force ejecuta miles de trampas de spam en todo el mundo y monitorea diariamente decenas de millones de ataques de spam y phishing mientras analiza miles de millones de páginas web e imágenes para detectar actividad fraudulenta y abuso de marca.

*"Si bien los registros vulnerados son una buena indicación de la actividad del ciberdelincuente, no cuentan la historia completa de 2017", dijo Wendi Whitmore, Líder Global del IBM X-Force Incident Response and Intelligence Services (IRIS). "El año pasado, hubo un claro enfoque por parte de los delincuentes para bloquear datos, no solo para robarlos, mediante ataques de ransomware. Estos ataques no se cuantifican por registros violados, pero han demostrado ser tan, o más, costosos para las organizaciones que una filtración tradicional. La capacidad de anticipar estos ataques y estar preparados será crítico ya que los ciberdelincuentes continuarán desarrollando sus tácticas para obtener mucho más dinero".*

### **Ataques de ransomware ejercen presión sobre las respuestas ante incidentes**

Los ataques de ransomware, como WannaCry, NotPetya y Bad Rabbit, no sólo acapararon los titulares en 2017, sino que también detuvieron a las principales organizaciones a medida que los cibercriminales tomaron el control y bloquearon la infraestructura crítica de salud, transporte y logística, entre otros. En general, los incidentes de ransomware han costado a las organizaciones más de USD \$8 mil millones en 2017, cuando los ciberdelincuentes lanzaron ataques que se centraron en bloquear datos críticos en lugar de comprometer los registros almacenados.

Esta tendencia aumenta la presión sobre las organizaciones para que estén preparadas adecuadamente con

estrategias de respuesta ante incidentes para limitar el impacto de un ataque. Un estudio de IBM Security, publicado el año pasado, encontró que una respuesta lenta puede afectar el costo de un ataque, ya que los incidentes que demoraron más de 30 días en contener cuestan USD \$1 millón más que los contenidos en 30 días.

### **El error humano sigue siendo un eslabón débil**

En 2017, los ciberdelincuentes continuaron aprovechando los errores humanos y los errores en las configuraciones de infraestructura para lanzar ataques. De hecho, el informe muestra que la actividad inadvertida, como la infraestructura de nube mal configurada, fue responsable de la exposición de casi el 70% de los registros comprometidos rastreados por IBM X-Force en 2017. El informe muestra que existe una conciencia creciente entre los ciberdelincuentes de la existencia de servidores en la nube mal configurados. Por ejemplo, en 2017 se produjo un aumento increíble del 424% en los registros vulnerados debido a errores de configuración en los servidores en la nube.

Más allá de la nube mal configurada, las personas atraídas por phishing representaron un tercio de la actividad inadvertida que condujo a un evento de seguridad en 2017. Esto incluye usuarios haciendo clic en un enlace o abriendo un archivo adjunto con código malicioso, generalmente compartido a través de una campaña de correo no deseado lanzada por ciberdelincuentes. El informe descubrió que en 2017, los ciberdelincuentes se basaron en gran medida en la botnet Necurs para distribuir millones de mensajes no deseados en sólo pocos días. Por ejemplo, durante un período de dos días en agosto, la investigación de IBM X-Force observó cuatro campañas separadas de Necurs enviando 22 millones de correos electrónicos.

### **Ciberdelincuentes encuentran éxito apuntando a clientes de servicios financieros**

En años pasados, los servicios financieros han sido la industria más atacada por los ciberdelincuentes. En 2017 cayó en el tercer puesto (17%) detrás de Tecnologías de la Información y Comunicación (33%) y Manufactura (18%), pero vio la mayoría de los incidentes de seguridad (27%) que requieren más investigación, en comparación con otras industrias.

Si bien las organizaciones de servicios financieros han invertido fuertemente en tecnologías de ciberseguridad para proteger a sus organizaciones, los ciberdelincuentes se centraron en aprovechar los troyanos bancarios dirigidos específicamente a los consumidores y usuarios finales.

Por ejemplo, el informe del IBM X-Force Threat Intelligence Index encontró que en 2017, el troyano bancario Gozi (y sus variantes) era el malware más utilizado contra la industria de servicios financieros. Este malware se dirige específicamente a los clientes, ya que se encarga de las pantallas de inicio de sesión bancarias con indicaciones para que los consumidores ingresen otra información personal que luego se comparte directamente con el atacante.

El uso de Gozi, considerado como una hábil operación del cibercrimen, pone de relieve cómo el crimen organizado está superando a todas las demás clases de actores en la escena del fraude facilitado por malware financiero.

El informe presenta datos recogidos por IBM entre el 1 de enero de 2017 y el 31 de diciembre de 2017, para brindar información detallada sobre el panorama global de amenazas e informar a los profesionales de seguridad sobre las amenazas más relevantes para sus organizaciones.

Para descargar una copia del IBM X-Force Threat Intelligence Index, visite: <https://www.ibm.com/account/reg/us-en/signup?formid=urx-31271>

Contacto(s)

**Susana Maldonado**

External Communications IBM México tel. (55) 5270 6502 [smaldona@mx1.ibm.com](mailto:smaldona@mx1.ibm.com)

**Fernanda Martínez**

External Communications IBM México (55) 4448 1923 [fer.martinez@mx1.ibm.com](mailto:fer.martinez@mx1.ibm.com)

---