IBM X-Force Research: la ciberdelincuencia abandona el ransomware para centrarse en criptojacking

Más de la mitad de los ataques ya no se hacen a través de malware Crecen las estafas a través de campañas de emails corporativos muy personalizados

Cambridge (Massachusetts) - 28 feb 2019: IBM Security ha anunciado hoy los resultados del índice anual de amenazas cibernéticas IBM X-Force Threat Intelligence Index, que desvela que las empresas están cada vez más concienciadas y emplean más medidas de seguridad para protegerse, lo que está impulsando a los ciberdelincuentes a modificar sus técnicas para obtener un mayor retorno de la inversión. El informe destaca dos cambios principales: una menor dependencia del malware y un sorprendente alejamiento del ransomware.

IBM X-Force ha observado una reducción significativa de ataques de ransomware. De hecho, los investigadores de IBM solo rastrearon una campaña de ransomware en 2018 desde la red de bots distribuidora de spam más grande del mundo, Necurs. IBM X-Force observó que, sin embargo, se multiplicó el cryptojacking -que consiste en utilizar la potencia de computación de una organización de forma ilegal y sin su conocimiento para hacer minería de criptomonedas- y que duplicó los ataques de ransomware. Al ser más rentable los ciberdelincuentes se están centrando en este tipo de ataque, ya que el precio de una criptomoneda como Bitcoin ha alcanzado en 2018 máximos de casi 20.000 dólares.

IBM X-Force descubrió también que los cibercriminales han modificado sus técnicas de ocultación. De hecho, según IBM X-Force, han aumentado los ataques de abuso del sistema operativo en detrimento del malware. Más de la mitad de los ataques cibernéticos (57%) utilizaban archivos infectados difíciles de detectar, incluido el uso de PowerShell y PsExe, mientras que el phishing representó casi un tercio (29%) de los ataques.

IBM X-Force se realiza a partir de la información obtenida a través de la monitorización de 70.000 incidentes de seguridad en más de 130 países. IBM X-Force ejecuta miles de trampas de spam en todo el mundo y monitoriza decenas de millones de ataques de spam y phishing a diario mientras analiza miles de millones de páginas web e imágenes para detectar actividades fraudulentas y abuso de marca. Otros de sus hallazgos son:

- Aumentan los informes de vulnerabilidades: Casi un tercio (42.000) de las 140.000 vulnerabilidades rastreadas por IBM X-Force en los últimos 30 años se reportaron en los últimos tres años. De hecho, IBM X-Force Red encuentra un promedio de 1.440 vulnerabilidades únicas, por organización.
- La mala configuración es una lacra frecuente en las empresas: los incidentes públicos por una mala configuración de los sistemas aumentaron un 20%. Curiosamente, el número de registros comprometidos se redujo en un 52%.
- Gran frecuencia de estafas realizadas a través de emails corporativos personalizados: las campañas de falsos correos electrónicos corporativos representaron el 45% del total de los ataques de phishing rastreados por X-Force.
- El transporte surge como una industria a tener en cuenta (para los atacantes cibernéticos): la industria del transporte se convirtió en el segundo sector más atacado en 2018, mientras que un año antes estaba en la décima posición.

La creciente conciencia sobre los problemas de seguridad cibernética y los controles de seguridad más estrictos están dificultando que los delincuentes cibernéticos establezcan puntos de apoyo en los sistemas objetivo. El resultado es que está disminuyendo el uso de software malicioso en los ataques. Más de la mitad (57%) de los ataques analizados por X-Force en 2018 reveló que los actores de amenazas no confiaban en el malware residente en el sistema de archivos. Cuando las redes se vieron comprometidas, IBM X-Force notó que los ciberdelincuentes abusaban de las herramientas de los sistemas

operativos existentes, en vez de utilizar malware para lograr sus objetivos. El núcleo de estas técnicas es el uso avanzado de PowerShell, una herramienta del sistema operativo capaz de ejecutar código desde la memoria y proporcionar acceso administrativo directamente al núcleo de un dispositivo.

Los ciberdelincuentes no son quienes gastan dinero de forma legítima en hardware costoso o en criptomonedas. Sin embargo, han desarrollado varias herramientas y tácticas para infectar tanto a servidores corporativos como a usuarios individuales con malware de minería de monedas para que hagan el trabajo por ellos. Estas infecciones secuestran la capcidad de cómputo, lo que resulta en un mayor uso de la CPU y dispositivos más lentos. Esta tendencia de cryptojacking está prácticamente explotando, y los ciberdelincuentes tienen la ventaja de que los dos vectores de infección más comunes son el phishing e inyectar códigos en sitios web con controles de seguridad débiles. IBM X-Force ha descubierto que los ataques ilícitos de cryptojacking están aumentando, mientras que el ransomware parece estar disminuyendo. En el transcurso de 2018, los intentos de instalar ransomware en dispositivos estudiados por X-Force en el cuarto trimestre (octubre-diciembre) disminuyeron a menos de la mitad (45%) respecto ll primer trimestre. En cambio, los ataques de cryptojacking se cuadruplicaron.

La industria del transporte es un objetivo creciente en materia de delitos informáticos

Los ciberdelincuentes no solo cambian la forma en que piratean, sino también a quién se dirigen La industria financiera siguió siendo el sector más atacado de 2018, y representó el 19% de todos los ataques observados por IBM X-Force IRIS. Sin embargo, la industria del transporte, que ni siquiera se ubicó en la lista de los 5 principales receptores de ataques el año pasado, se trasladó al segundo sector en 2018. El informe presenta datos que IBM recopiló entre el 1 de enero de 2018 y el 31 de diciembre de 2018 para brindar información detallada sobre el panorama de amenazas globales e informar a los profesionales de seguridad sobre las amenazas más relevantes para sus organizaciones.

Para descargar una copia del Índice de amenazas de IBM X-Force 2019, pincharaquí.

Acerca de IBM Security

IBM Security ofrece una de las carteras más avanzadas e integradas de productos y servicios de seguridad empresarial. El portafolio, respaldado por la investigación de IBM X-Force® de renombre mundial, permite a las organizaciones administrar de manera efectiva los riesgos y defenderse contra amenazas emergentes. IBM opera una de las organizaciones de investigación, desarrollo y entrega de seguridad más amplias del mundo, supervisa 70 mil millones de eventos de seguridad por día en más de 130 países y se le han otorgado más de 10.000 patentes de seguridad en todo el mundo. Para obtener más información, visite www.ibm.com/security, siga @IBMSecurity en Twitter o visite el blog deIBM Security Intelligence.

Contacto(s)

Patricia Núñez Canal

IBM Comunicación Externa +34 91 3977782 patricia.nunez@es.ibm.com