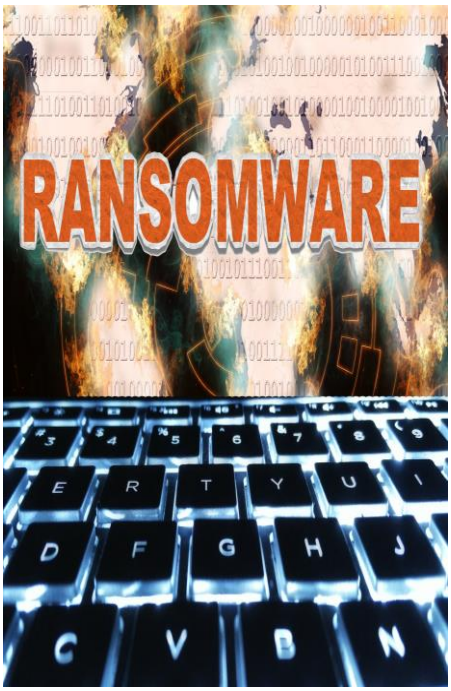
05/08/22

Los ataques de ransomware conocidos apenas supondrían una sexta parte del total



El ransomware, una de las principales amenazas informáticas a escala mundial, ha experimentado en los últimos años un crecimiento insólito.

Algunos sucesos notables, según la importancia de las organizaciones afectadas o de los datos comprometidos, llegan a la prensa y el gran público. Sin embargo, una proporción significativa de los ataques escapa todavía a los equipos de investigación y las autoridades, una ceguera informativa que entorpece la lucha contra una plaga que perjudica cada año a cientos de empresas de todos los sectores profesionales.

El informe “ENISA Thread Landscape for Ransomware Attacks”, de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), se basa en el estudio de 623 incidentes dados a conocer entre mayo de 2021 y junio de 2022, y que involucraron a entidades especialmente de la Unión Europea, el Reino Unido y Estados Unidos. Se propone una estimación de 3640 ataques ocurridos en el periodo considerado, por lo que los sucesos analizados constituirían el 17,11 % del total. La “punta del iceberg”, como se denota en el propio texto, pone de manifiesto la falta de estadísticas y análisis fiables y detallados relativos a esta área, en buena parte por la reticencia de las compañías a colaborar con las autoridades y agencias de seguridad. El temor a posibles represalias de los ciberdelincuentes o el daño a su reputación que supondría una exposición pública, ya se trate del hecho de haber sufrido una intrusión o de sus detalles y la naturaleza de información comprometida, se señala como el factor determinante. En consecuencia, la mayoría de los incidentes pasa desapercibida o no queda suficientemente acreditada y la documentación de la que se dispone respecto a otros permanece incompleta en muchos casos.

Las entidades que intentan por su cuenta satisfacer el rescate o pactar con los ciberdelincuentes unas condiciones más favorables, sin comunicarlo a nadie, no siempre logran recuperar los datos cifrados o sustraídos, ni evitar que se filtren en parte o en su totalidad. El informe subraya la absoluta inconveniencia de esta práctica, que estimula la

continuidad de las operaciones de los grupos de ransomware y contribuye a su consolidación, al tiempo que priva de testimonios, pruebas y recursos técnicos valiosos a los investigadores.

Otras conclusiones relevantes

Debido a la propia selección de los incidentes analizados, las limitaciones sobre la información disponible y la fiabilidad en ocasiones escasa de las fuentes consultadas, los datos cuantitativos presentados exhiben un cierto grado de sesgo e incertidumbre.

1. Aproximadamente se filtraron de media 10 terabytes de datos cada mes. La información personal de los empleados constituyó el 58,2 % del total.
2. Se identificaron 47 grupos de ransomware diferentes, con la preponderancia de Conti y LockBit.
3. Se desconoce en la inmensa mayoría de incidentes, casi el 95 %, si la empresa afectada pagó o no el rescate exigido. Dado que los operadores de ransomware suelen exponer a las víctimas que no han cedido a sus chantajes, lo que tiende a ocurrir en 4 de cada 10 ataques, se sugiere que en el resto de casos hubo un acuerdo o las compañías encontraron otra vía de solución.
4. No hay discriminación aparente por sectores: desde la industria pesada hasta entidades gubernamentales, pasando por finanzas, moda, transportes o entretenimiento.
5. Tan solo 29 de los incidentes estudiados confirman el método de acceso a los sistemas de las empresas afectadas: escritorios remotos expuestos o poco protegidos, phishing a empleados, credenciales robadas, aprovechamiento de vulnerabilidades de software y compromiso de la cadena de suministro. Los investigadores consideran fundamental este aspecto para ayudar a mejorar la protección de otras entidades antes de que se conviertan en nuevas víctimas.

El informe propone una serie de consejos para prepararse ante los incidentes de ransomware y mitigar en la medida de lo posible sus efectos devastadores, como el mantenimiento adecuado de las copias de seguridad, la aplicación de actualizaciones de software, la segmentación de las redes o una correcta gestión de credenciales y privilegios. También se insiste, en caso de resultar objeto de un ataque, en contactar con las autoridades y las agencias de seguridad para recibir asesoramiento, no pagar rescates ni negociar con los ciberdelincuentes, y poner en cuarentena los sistemas afectados.