Ante el Ransomware 2.0 las empresas deben actuar antes de que sea demasiado tarde: Tanium

Ciudad de México. 10 de noviembre de 2022.- Tanium, proveedor líder de la industria de administración convergente de terminales (XEM) de la industria, alertó que el ransomware ha adquirido un riesgo aún mayor con el denominado ransomware 2.0, con el que los ciberatacantes ya no solo cifran archivos y piden rescate, sino que amenazan con filtrar la información que pueden robar y distribuirla por Internet, por lo que todas las organizaciones deben considerarse un objetivo potencial ante esta amenaza y construir una defensa eficaz antes de que sufran un incidente.

El ransomware 2.0 es una variante del ransomware tradicional que busca atacar de diferente forma, ya que hasta hace poco el ransomware únicamente cifraba archivos y sistemas para pedir un rescate a cambio a través de esta estrategia maliciosa. El ransomware se ha convertido en una de las amenazas más comunes y de mayor impacto en el panorama de la ciberseguridad. El costo y la frecuencia de estos ataques son crecientes y todas las industrias han sufrido incidentes de alto perfil.

De esta manera, Tanium alerta que esta amenaza puede afectar a usuarios particulares y principalmente, a empresas, ya que los ciberdelincuentes piden un rescate económico a cambio de no distribuir toda la información en la red, entre la competencia o a cualquier persona en Internet.

“La técnica más utilizada es el phishing para engañar a las víctimas, que pueden ser empleados de una empresa, para que hagan clic en un enlace o entren en determinada página para de esa forma lograr que descargue o instale un software malicioso que es el ransomware y la puerta de entrada, por lo que lo mejor siempre será prevenir este tipo de amenazas y no comprometer los sistemas y equipos”, señaló Miguel Llerena, vicepresidente para Latinoamérica de Tanium.

Con el aumento del cibercrimen y los ataques como el ransomware, cualquier empresa o institución debe reflexionar si ha hecho copias de seguridad de todos los datos críticos y comprobado si se puede acceder a ellos fácilmente, en caso de que se produzca una brecha de seguridad y, asimismo, si ha incluido las copias de seguridad como parte de sus esfuerzos de ciberhigiene y estrategia de seguridad.

La empresa indica que este tema debe de tomarse en serio porque en muchos casos las organizaciones no realizan sus backup de forma eficaz y esto es alarmante porque si sufren una violación de datos, el impacto sería muy perjudicial. Las copias de seguridad son a menudo la última línea de defensa contra los ciberataques y ofrecen un salvavidas crucial si no se pueden recuperar los sistemas.

Tanium informó que en los últimos años, todas las industrias han experimentado importantes infracciones de ransomware: cuidado de la salud, gobierno, educación,

tecnología, retail. Nadie está a salvo. Toda organización debe verse como un objetivo potencial de los ciberatacantes y construir defensas efectivas contra este patrón de ataque antes de que se convierta en la siguiente víctima.

Una encuesta reciente de Tanium reveló:

- 3/4 de las empresas invierten en ciberseguridad después de ser atacadas.
- 63% de los líderes están preocupados por la ciberseguridad después de un incidente.
- El 79% de los líderes aprueban un presupuesto de ciberseguridad después de una violación de datos.
- El 55% no cuenta con suficientes empleados para adoptar medidas preventivas de seguridad.

De acuerdo al estudio, el 92% de las empresas han sufrido un ataque o brecha de datos, sólo en el último año. Muchos de estos ataques son robos de información en el que requieren el pago en Bitcoin para recuperar los datos. Esta encuesta confirmó que la actividad cibernética maliciosa sigue siendo común.

El panorama está empeorando para los defensores, señala el estudio: más de dos tercios (69%) admitieron que las amenazas están aumentando y esperan que en 2022 se registre la mayor cantidad de ataques de la historia.

Una solución de seguridad moderna contra el ransomware

La plataforma de Tanium fue diseñada para ayudar a proteger los entornos modernos ya que adopta un enfoque diferente en comparación con las estrategias actuales de la mayoría de las organizaciones porque aborda los desafíos que enfrentan las organizaciones al utilizar su legado de herramientas para así asegurar y administrar sus entornos.

“Es una plataforma unificada que ofrece la mayor parte del núcleo de capacidades requeridas para detectar, investigar y remediar amenazas de ransomware en una sola herramienta. Estas capacidades funcionan y operar a partir de los mismos datos e impulsan una colaboración de respuesta a las amenazas, eliminando al mismo tiempo, la complejidad de implementar multiples herramientas”, agregó Llerena.