Tanium previene de la extorsión doble y triple de ransomware

Ciudad de México. 26 de enero de 2023.- Tanium, proveedor líder de la industria de administración convergente de terminales (XEM) de la industria, señala que tras ser golpeada por un ataque de ransomware, en muchos casos, los delincuentes aún tratan de extorsionar a una empresa no obstante haya pagado el rescate. Las extorsiones dobles e incluso triples son cada vez más comunes y los ciberdelincuentes ahora exigen pagos adicionales para evitar que se filtre la información privada capturada en sus ataques.

En los ataques de ransomware tradicionales, los atacantes secuestran y cifran datos valiosos para obligar a las organizaciones a pagar un rescate a cambio de la restauración segura de los datos y la funcionalidad de la red. Los CISO (Chief Information Security Officer) han respondido adoptando protecciones cibernéticas más sólidas, como la creación de copias de seguridad externas seguras y la segmentación de sus redes, no obstante los atacantes han evolucionado rápidamente para superar estos métodos de administración.

Una extorsión, dos extorsiones, tres

Durante el último año, los atacantes se dieron cuenta del valor que las organizaciones otorgan a no divulgar su información confidencial públicamente: el impacto en la marca y la reputación a veces puede ser tan dañino como el bloqueo, tener archivos y sistemas expuestos. Aprovechando lo anterior, los atacantes comenzaron a agregar la amenaza de filtrar datos confidenciales como seguimiento de ataques de ransomware exitosos o incluso fallidos cuando las organizaciones podían usar copias de seguridad para restaurar sus sistemas.

Con la doble extorsión siendo tan exitosa, los atacantes no se detuvieron ahí y, en casos de triple extorsión, los atacantes amenazan con divulgar datos sobre socios y clientes intermedios para extraer pagos de rescate adicionales, lo que podría poner a la organización inicial en riesgo de demandas o multas.

“La única defensa real contra la doble y triple extorsión es asegurarse de que los atacantes no tengan acceso a la información más confidencial. La principal prioridad debe ser categorizar los datos críticos para que, cuando los ciberdelincuentes superen las primeras líneas de defensa, no puedan robar los elementos más valiosos. Este proceso de supervisión implica restringir el acceso a los datos y a las herramientas que interactúan directamente con ellos”, externó Miguel Llerena, vicepresidente para Latinoamérica de Tanium.

Tanium señala que cuantos menos puntos de acceso, más fácil será proteger los datos y hace algunas recomendaciones:

- Saber dónde se ubican los datos y adoptar soluciones con alertas en tiempo real que muestren cuándo se guardan, transfieren o almacenan datos confidenciales de forma insegura. Cuando se enfocan los esfuerzos en proteger la información más crítica, ayuda a limitar las alertas y se determina exactamente quién y qué interactúa con esos datos.

- Mantenerse informados de los riesgos dinámicos asociados con los nuevos dispositivos que ingresan a una red cuando los empleados se incorporan o cuando los dispositivos asociados con exempleados deben tener acceso o se deben eliminar las credenciales.

- Establecer una comprensión básica del "comportamiento normal" en el entorno para detectar cuando algo adverso o anormal está en proceso.

Si aún con lo anterior se experimenta una violación de seguridad, hay que asegurarse de limitar las posibilidades de los atacantes de acceder a datos privados:

- Cambiar de forma controlada las contraseñas usadas que puedan estar asociadas con sistemas comprometidos.

- Verificar que la información de la infracción provenga de una fuente legítima, ya que los correos electrónicos comprometidos pueden parecer oficiales cuando en realidad son fraudulentos.

- Garantizar que los esfuerzos de recuperación vayan más allá de "borrar y volver a generar imágenes" para incluir verificaciones exhaustivas que encuentren signos residuales que estuvieran comprometidas.

- Identificar los puntos de acceso iniciales que fueron violados para evitar la reintroducción del vector de ataque durante los esfuerzos de recuperación.

“Los efectos paralizantes de un ataque de ransomware pueden ser devastadores para cualquier negocio. Pero ahora hay mucho más en juego debido a la superficie de ataque ampliada que amenaza el ecosistema extendido de socios, clientes e inversores de una empresa. Como resultado, todas las organizaciones deben desarrollar un plan de acción para defender sus datos y protegerse no solo de los ataques iniciales de ransomware, sino también de las maniobras dobles y triples de ransomware”, concluyó Llerena.