La pandemia de COVID-19 ha tenido un efecto dramático en las organizaciones a nivel mundial. Como se informó anteriormente, *los* actores de amenazas *siempre* buscarán aprovechar los eventos o cambios importantes para su propio beneficio. La pandemia de COVID-19 presentó a los ciberdelincuentes la oportunidad perfecta para aprovechar el interés de los medios globales para difundir actividades maliciosas. Hemos encontrado que los dominios temáticos-Coronavirus son un 50% más probabilidades de ser malicioso y que ha habido más de 2.600 ataques cotidianos en relación con la pandemia. Además, las nuevas campañas de phishing se hicieron pasar por la OMS y las plataformas de conferencias populares para robar información confidencial, alcanzando un máximo de 192,000 ciberataques relacionados con el coronavirus por semana.

La 'Nueva normalidad' ahora significa ciberataques Gen V

Los actores de amenazas se han vuelto muy sofisticados. La última generación de ciberataques presenta un juego de pelota completamente diferente, ya que los ciberataques sofisticados están aumentando no solo en volumen sino también en impacto, complejidad y velocidad. Los piratas informáticos están evolucionando constantemente su tecnología y técnicas para distribuir malware de forma creativa. Anteriormente proyectamos que la pandemia desaparecerá, pero su efecto cibernético no lo hará. Esto ahora se ha convertido en una realidad.

Aumento de ransomware

Las organizaciones de todo el mundo están experimentando un aumento masivo de los ataques de ransomware . En el tercer trimestre de 2020, hubo un aumento del 50% en el promedio diario de ataques de ransomware, en comparación con la primera mitad del año.

Si bien algunos ataques reportados fueron llevados a cabo por cadenas de ransomware conocidas como REvil y Ryuk , varias grandes corporaciones experimentaron ataques completos utilizando una variante previamente desconocida, **Pay2Key** .

Pay2Key se propaga rápidamente a través de las redes de las víctimas, dejando partes significativas de la red encriptadas con una nota de rescate que amenaza con filtrar datos corporativos robados a menos que se pague el rescate.

Ryuk, el infame ransomware, también apuntó a hospitales en lo que se consideró como una ola de ataques dirigidos contra la industria de la salud. El CISA, el FBI y el HHS emitieron una advertencia contra los ataques de ransomware en hospitales de EE. UU., Diciendo que tienen información creíble de una amenaza creciente e inminente de delitos cibernéticos. Octubre vio un aumento del 71% en los ataques de ransomware contra el sector de la salud en los EE. UU. Los ataques de ransomware también aumentaron un 33% en APAC y un 36% en EMEA.

Recomendaciones para prevenir la próxima ciberpandémica

PREVENCIÓN EN TIEMPO REAL

Como hemos aprendido, la vacunación es mucho mejor que el tratamiento. Lo mismo se aplica a su seguridad cibernética. La prevención en tiempo real coloca a su organización en una mejor posición para defenderse de la próxima pandemia cibernética. .

Las organizaciones que hacen hincapié en la prevención de amenazas desconocidas de día cero pueden ganar la batalla de la seguridad cibernética.

ASEGURA TU TODO

Cada parte de la cadena es importante. Su nueva normalidad requiere que revise y verifique el nivel de seguridad y la relevancia de las infraestructuras de su red, los procesos, el cumplimiento de dispositivos móviles conectados, terminales e IoT .

El mayor uso de la nube significa un mayor nivel de seguridad, especialmente en tecnologías que protegen cargas de trabajo, contenedores y aplicaciones sin servidor en entornos de nubes múltiples e híbridas.

CONSOLIDACIÓN Y VISIBILIDAD

El nivel más alto de visibilidad, alcanzado a través de la consolidación, le garantizará la efectividad de seguridad necesaria para prevenir ciberataques sofisticados. La gestión unificada y la visibilidad de los riesgos completan su arquitectura de seguridad. Esto se puede lograr reduciendo sus proveedores y soluciones de productos puntuales, y sus costos generales.

MANTENGA SU INTELIGENCIA DE AMENAZAS ACTUALIZADA

La inteligencia de amenazas combina información de múltiples fuentes, proporcionando una pantalla de protección más efectiva para su red. Para mantener las operaciones comerciales, necesita inteligencia integral para detener de manera proactiva las amenazas, administración de servicios de seguridad para monitorear su red y respuesta a incidentes para responder y resolver Ataques.