5 **Elimine las Cargas Iniciales de en el Gateway.** Los firewalls como Firebox de WatchGuard tienen buenas posibilidades de bloquear archivos de malware de primera etapa, como instaladores, a los que con frecuencia siguen elementos más maliciosos. Firebox ofrece tres niveles de protección contra malware: Gateway AV (firmas y heurística), IntelligentAV (prevención sin firma con tecnología de IA) y APT Blocker (sandbox en la nube avanzado).

6 **Supervise los Ataques Activos con Visibilidad en Tiempo Real.** Por naturaleza, el ransomware infecta los dispositivos de endpoint. Tener visibilidad de la actividad de evento de estos dispositivos permite la detección y corrección de las amenazas antes de que se produzca el daño. Adaptive Defense 360 proporciona visibilidad clara y oportuna de la actividad maliciosa en toda la organización. Esta visibilidad permite a los equipos de seguridad evaluar rápidamente el alcance de un ataque y adoptar las respuestas adecuadas.

7 **Correlacione la Telemetría para Obtener un Contexto Más Amplio.** Los criminales informáticos son ninjas que evitan los sistemas de seguridad tradicionales. Utilizan ataques sigilosos y dirigidos para no dejar huellas y ocultarse en las sombras, de modo que es muy difícil detectarlos. Nuestra solución ThreatSync, que forma parte de Firebox de WatchGuard, utiliza un sensor de host liviano y la potencia de la nube para correlacionar automáticamente datos telemétricos de diferentes puntos de la pila de seguridad a fin de detectar y desactivar rápidamente amenazas que habrían pasado inadvertidas.

8 **Detenga el Cifrado de Archivos sin Mover un Dedo.** Host Ransomware Prevention (HRP) aprovecha el motor de análisis de comportamiento y un honeypot de directorios señuelo para supervisar una gran cantidad de características que determinan si cierta acción está o no asociada con un ataque de ransomware. Si se determina que la amenaza es maliciosa, el HRP puede prevenir un ataque de ransomware automáticamente, antes de que se realice el cifrado de los archivos en el endpoint.

9 **Restaure los Endpoints con Facilidad.** Durante la ejecución, a menudo, el malware crea, modifica o elimina ajustes del registro y archivos del sistema, y modifica la configuración de los ajustes. Estos cambios, o sus remanentes, pueden provocar el mal funcionamiento o la inestabilidad del sistema o, incluso, ser una puerta abierta para nuevos ataques. En estos casos residuales en los que el malware tiene permiso para ejecutarse, Adaptive Defense 360 restaura los endpoints a su estado de confianza anterior al malware.

10 **Minimice el Tiempo de Detección.** El Threat Hunting and Investigation Service de WatchGuard ayuda a detectar técnicas emergentes de ataques informáticos y living-off-the-land. Con la ayuda de nuestros expertos en seguridad, analizamos casos sospechosos en busca de técnicas de evasión novedosas y únicas en el flujo de eventos. En función de esto, creamos reglas que representan nuevos IoA (indicadores de ataque) que se pueden implementar en los endpoints para protegerlos rápidamente contra nuevos ataques.

DIAGONAL INFORMÁTICA

1. https://www.darkreading.com/risk/average-ransomware-payments-more-than-doubled-in-q4-2019/d/d-id/1336893
2. https://www.natlawreview.com/article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion
3. https://www.scribd.com/document/320027570/Malwarebytes
4. https://www.businesswire.com/news/home/20191016005043/en/Cost-Ransomware-Related-Downtime-Increased-200-Percent
5. http://webroot-cms-cdn.s3.amazonaws.com/7814/5617/2382/Webroot-2016-Threat-Brief.pdf
6. http://labs.lastline.com/lastline-labs-av-isnt-dead-it-just-cant-keep-up
7. https://www.av-test.org/en/statistics/malware/

ACERCA DE WATCHGUARD

WatchGuard® Technologies, Inc. es un líder mundial en seguridad de red, seguridad de endpoint, Wi-Fi seguro, autenticación multifactor y servicios de inteligencia de red. Más de 18.000 revendedores de seguridad y proveedores de servicios de todo el mundo confían en los productos y los premiados servicios de la empresa para proteger a 250.000 clientes. La misión de WatchGuard es lograr que empresas de todos los tipos y tamaños accedan de manera sencilla a una seguridad de calidad empresarial. Por ello, WatchGuard es una solución ideal para medianas empresas y también para empresas distribuidas. La empresa tiene su oficina central en Seattle, Washington, y posee oficinas en Europa, la región de Asia-Pacífico, Latinoamérica y otras regiones de Norteamérica. Para obtener más información, visite WatchGuard.com.

Para obtener información adicional, promociones y actualizaciones, siga a WatchGuard en Twitter @WatchGuard, en Facebook o en la página de nuestra empresa en LinkedIn. Además, visite nuestro blog de seguridad de la información, Secplicity, para obtener información en tiempo real sobre las amenazas más recientes y sobre cómo lidiar con ellas en www.secplicity.org.

VENTAS EN MEXICO +52.55.5347.6063 VENTAS ESPAÑA +34.917.932.531 www.watchguard.com/es

No se proporcionan garantías expresas ni implícitas. Todas las especificaciones están sujetas a cambios y todas las funcionalidades, las características o los productos futuros previstos se suministrarán según su disponibilidad. ©2021 WatchGuard Technologies, Inc. Todos los derechos reservados. WatchGuard, el logotipo de WatchGuard, Fireware, Firebox, ThreatSync e IntelligentAV son marcas comerciales o marcas comerciales registradas de WatchGuard Technologies, Inc. en los Estados Unidos y/o en otros países. Los demás nombres comerciales son propiedad de sus respectivos dueños. N.º de pieza WGCE66990_071221