La investigación de WatchGuard encuentra un aumento del 12% en las amenazas evasivas

WatchGuard Technologies, referente en seguridad e inteligencia de redes, Wi-Fi seguro, autenticación multifactor y protección avanzada de terminales, anunció hoy el lanzamiento de su Informe de seguridad de Internet para el segundo trimestre de 2020.

Entre sus más importantes hallazgos el informe mostró que a pesar de una **disminución del 8% en las detecciones generales de malware** en el segundo trimestre, el 70% de todos los ataques involucraron malware de día cero (variantes que eluden las firmas de antivirus), lo que representa un aumento del 12% con respecto al trimestre anterior.

"Las empresas no son las únicas que han ajustado sus operaciones debido a la pandemia global de COVID-19; los ciberdelincuentes también lo han hecho", dijo **Corey Nachreiner, Director de Tecnología de WatchGuard**. "El aumento de los ataques bien planeados, a pesar del hecho de que las detecciones generales de malware disminuyeron en el segundo trimestre (probablemente debido al cambio al trabajo remoto), muestra que los atacantes están recurriendo a tácticas más evasivas y efectivas que las defensas antimalware tradicionales, basadas en firmas, simplemente no pueden capturar. Todas las organizaciones deben priorizar la detección de amenazas basada en el comportamiento, el espacio aislado en la nube y un conjunto de servicios de seguridad en capas para proteger tanto la red central como las fuerzas de trabajo remotas".

El **Informe de seguridad de Internet de WatchGuard** ofrece una visión detallada de las últimas tendencias de ataques de red y malware, una investigación en profundidad de amenazas y las mejores prácticas de seguridad recomendadas que las organizaciones pueden aprovechar para protegerse mejor a sí mismas, a sus socios y clientes.

Los hallazgos clave del informe del segundo trimestre de 2020 incluyen:

- **Los atacantes continúan aprovechando las amenazas evasivas y cifradas**: el malware de día cero representó más de dos tercios de las detecciones totales en el segundo trimestre, mientras que los ataques enviados a través de conexiones HTTPS cifradas representaron el 34%. Las organizaciones que no pueden inspeccionar el tráfico cifrado perderán un tercio de las amenazas entrantes. Aunque el porcentaje de amenazas que utilizan cifrado disminuyó del 64% en el primer trimestre, el volumen de malware cifrado con HTTPS aumentó drásticamente. Parece que más administradores están tomando los pasos necesarios para habilitar la inspección HTTPS en los dispositivos de seguridad Firebox, pero aún hay más trabajo por hacer.
- **Los ataques basados en JavaScript están en aumento**: el script de estafa Trojan.Gnaeus hizo su debut en la parte superior de la lista de los 10 principales malware de WatchGuard para el segundo trimestre, representando casi una de cada cinco detecciones de malware. El malware Gnaeus permite a los actores de amenazas

secuestrar el control del navegador de la víctima con código ofuscado y redirigir, a la fuerza, lejos de sus destinos web previstos a dominios bajo el control del atacante. Otro ataque de JavaScript de estilo emergente, J.S. PopUnder, fue una de las variantes de malware más extendidas el último trimestre. En este caso, un script ofuscado escanea las propiedades del sistema de la víctima y bloquea los intentos de depuración como táctica anti-detección. Para combatir estas amenazas, las organizaciones deben evitar que los usuarios carguen una extensión del navegador de una fuente desconocida, mantener los navegadores actualizados con los últimos parches, usar adblockers de buena reputación y mantener un motor anti-malware actualizado.

- **Los atacantes utilizan cada vez más archivos de Excel cifrados para ocultar malware**: XML-Trojan. Abracadabra es una nueva incorporación a la lista de las 10 principales detecciones de malware de WatchGuard, que muestra un rápido crecimiento en popularidad desde que surgió la técnica en abril. Abracadabra es una variante de malware que se entrega como un archivo de Excel cifrado con la contraseña "VelvetSweatshop" (la contraseña predeterminada para los documentos de Excel). Una vez abierto, Excel descifra automáticamente el archivo y un script de macro VBA dentro de la hoja de cálculo se descarga y ejecuta un ejecutable. El uso de una contraseña predeterminada permite que este malware eluda muchas soluciones antivirus básicas, ya que el archivo está cifrado y luego descifrado por Excel. Las organizaciones nunca deben permitir macros de una fuente que no sea de confianza y aprovechar el espacio aislado en la nube para verificar de manera segura la verdadera intención de los archivos potencialmente peligrosos antes de que puedan causar una infección.

- **Un antiguo ataque DoS altamente explotable regresa**: una vulnerabilidad de negación de servicio (DoS) de hace seis años que afecta a WordPress y Drupal apareció en la lista de WatchGuard de los 10 principales ataques de red por volumen en el segundo trimestre. Esta vulnerabilidad es particularmente grave porque afecta a todas las instalaciones de Drupal y WordPress sin parches y crea escenarios de DoS en los que los malos actores pueden causar el agotamiento de la CPU y la memoria en el hardware subyacente. A pesar del alto volumen de estos ataques, estaban hiperconcentrados en unas pocas docenas de redes principalmente en Alemania. Dado que los escenarios de DoS requieren un tráfico sostenido a las redes de las víctimas, esto significa que existe una gran probabilidad de que los atacantes seleccionaran sus objetivos intencionalmente.
- **Los dominios de malware aprovechan los servidores de comando y control para causar estragos**: dos nuevos destinos se incluyeron en la lista de dominios de malware más importantes de WatchGuard en el segundo trimestre. El sitio más común fue findresults [.], Que usa un servidor C&C para una variante del troyano Dadobra que crea un archivo ofuscado y un registro asociado para garantizar que el ataque se ejecute y pueda filtrar datos confidenciales y descargar malware adicional cuando los usuarios inician sistemas Windows. Un usuario alertó al equipo de WatchGuard sobre Cioco-froll [.] Com, que utiliza otro servidor C&C para admitir una variante de botnet Asprox (a menudo entregada a través de un documento PDF) y proporciona una baliza C&C para que el atacante sepa que ha ganado persistencia y está listo participar en la botnet. El firewall DNS puede ayudar a las organizaciones a detectar y bloquear este tipo de amenazas independientemente del protocolo de aplicación para la conexión.

Los informes de investigación trimestrales de WatchGuard se basan en datos anónimos de Firebox Feed de dispositivos WatchGuard activos cuyos propietarios han optado por compartir datos para respaldar los esfuerzos de investigación de Threat Lab. En el segundo trimestre, casi 42.000 dispositivos WatchGuard contribuyeron con datos al informe, bloqueando un total de más de 28,5 millones de variantes de malware (684 por dispositivo) y más de 1,75 millones de amenazas de red (42 por dispositivo). Los dispositivos Firebox detectaron y bloquearon colectivamente 410 firmas de ataques únicos en el segundo trimestre, un aumento del 15% con respecto al primer trimestre y la mayor cantidad desde el cuarto trimestre de 2018.

El informe completo incluye más información sobre las principales tendencias de redes y malware que afectan a las empresas medianas en la actualidad, así como las estrategias de seguridad recomendadas y las mejores prácticas para defenderse de ellas. El informe también incluye un análisis detallado de la reciente ola de violaciones de datos provocada por el grupo de piratería ShinyHunters.