Investigadores de seguridad cibernética de Intego advierten sobre la posible explotación activa de una vulnerabilidad de seguridad que no ha sido parcheada, en los detalles de las características de seguridad de MacOS Gatekeeper de Apple y el PoC, que se dio a conocer públicamente a finales del mes pasado.

La semana pasada, el equipo de Intego descubrió cuatro muestras de nuevo malware de MacOS en VirusTotal que aprovechan la vulnerabilidad de omisión de Gatekeeper para ejecutar código no confiable en MacOS sin mostrar a los usuarios ninguna advertencia o pedir su permiso explícitamente.

Sin embargo, el malware recién descubierto, denominado como OSX/Linker, no se ha visto activo hasta el momento y parece estar en desarrollo. A pesar de que las muestras aprovechan el defecto de desvío de Gatekeeper no parcheado, no descargan ninguna aplicación maliciosa del servidor del atacante.

Según Joshua Long, de Intego, hasta la semana pasada, *«el fabricante de malware simplemente estaba realizando un reconocimiento de pruebas de detección».*

> *«Uno de los archivos fue firmado con una ID de desarrollador de Apple, es evidente que las imágenes de disco OSX/Linker son obra de los desarrolladores del adware OSX/Surfbuyer»,* dijo Long en una publicación.

Pero ya que la muestra de malware se vincula a un servidor remoto desde donde descarga la aplicación que no es de confianza, los atacantes también pueden distribuir las mismas muestras al objetivo real simplemente reemplazando la aplicación de muestra definida con una aplicación de malware en su servidor.

Vulnerabilidad de omisión del controlador de acceso a MacOS

GateKeeper es una característica de seguridad integrada en Apple MacOS que impone la firma del código y verifica las aplicaciones descargadas antes de permitir que se ejecuten, lo

que ayuda a los usuarios a proteger sus sistemas contra malware y otros programas maliciosos.

Esto significa que al descargar una aplicación de Internet, GateKeeper solo permitirá que se ejecute sin ninguna advertencia si se ha firmado con un certificado válido emitido por Apple, de lo contrario le solicitará que permita o deniegue la ejecución.

Sin embargo, GateKeeper ha sido diseñado para tratar las unidades externas USB o HDD, y los recursos compartidos de red como *«ubicaciones seguras»* desde donde los usuarios pueden ejecutar cualquier aplicación sin involucrar las verificaciones y avisos de GateKeeper.

Filippo Cavallarin, un investigador de seguridad independiente, a fines del mes pasado reveló públicamente una forma de explotar este comportamiento al combinarlo con otras dos características legítimas del sistema operativo MacOS:

Los archivos zip pueden contener enlaces simbólicos que apuntan a una ubicación arbitraria, incluidos los puntos finales de automount, y la función de montaje automático en MacOS puede montar automáticamente un recurso compartido de red desde un servidor remoto simplemente accediendo a él con una ruta «especial», es decir, que comience con «/net/».

> *«Por ejemplo, /net/evil-attacker.com/sharefolder/ hará que el sistema operativo lea el contenido de la «carpeta compartida» en el host remoto usando NFS»,* explicó Cavallarin.

Como se muestra en el video, Cavallarin creó un archivo ZIP con un enlace simbólico a un recurso compartido de red controlado por un atacante que MacOS montará automáticamente.

Una vez que la víctima abre el archivo ZIP y sigue el enlace, navegará a la red compartida controlada por el atacante en la que confía el controlador de acceso, engañando a la víctima para que ejecute archivos maliciosos sin ninguna advertencia.

> *«La forma en que está diseñado el Finder (por ejemplo las extensiones ocultas .app, ocultar la ruta completa de la barra de título), hace que esta técnica sea muy efectiva y difícil de detectar»*, dijo el investigador.

Sin embargo, las muestras de malware recién descubiertas no son archivos ZIP, sino archivos de imagen de disco, lo que demuestra que *«los fabricantes de malware estaban experimentando para ver si la vulnerabilidad de Cavallarin también funcionaría con las imágenes de disco».*

Cavallarin informó responsablemente sus hallazgos a Apple el 22 de febrero, pero decidió hacerlo público a fines del mes pasado luego de que la compañía no pudo solucionar el problema dentro del plazo de 90 días para la divulgación y comenzó a ignorar sus correos electrónicos.

Hasta que Apple solucione el problema, el investigador recomendó a los administradores de red bloquear las comunicaciones de NFS con direcciones IP externas y, para los usuarios domésticos, siempre es importante no abrir archivos adjuntos de correo electrónico de una fuente desconocida, sospechosa o poco confiable.