
Alerta de Seguridad Informática (2CMV-00014-001)

Nivel de Riesgo: Alto

Tipo: Informe Ransomware Ryuk

Fecha de lanzamiento original: 05 de julio de 2019 | Última revisión 05 de Julio de 2019

Notificación

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), disponibiliza a la comunidad el siguiente informe sobre el Ransomware Ryuk.

Descripción General de un Ransomware

Un Ransomware es un tipo de software malicioso o malware, diseñado para denegar el acceso a una data o a los sistemas computacionales hasta que la víctima realice un pago para retomar el control de los mismos.

Los Ransomware normalmente son propagados mediante correos de phishing o a través de sitios web infectados.

Las consecuencias de un Ransomware pueden ser devastadoras para las personas y las organizaciones. Todos quienes almacenan información de gran relevancia en sus computadores o redes puede estar en riesgo, incluyendo gobiernos nacionales y locales, empresas públicas y privadas, entidades financieras, sistemas de salud, sistemas de comunicaciones, industrias u otra clase de infraestructuras críticas.

La recuperación de la data puede ser un proceso difícil y costoso, que requiere el servicio de especialistas con reputación. Algunas víctimas de Ramsonware toman la decisión de pagar lo exigido

por los cibercriminales para recuperar sus archivos, sin embargo, no existe garantía de que los individuos o entidades recuperen la información secuestrada una vez pagado el rescate.

Ransomware Ryuk

Ryuk fue descubierto en Agosto de 2018 y desde entonces ha sido responsable de múltiples ataques a nivel global.

Ryuk es un Ransomware diseñado para realizar ataques dirigidos, los que realiza de acuerdo a la capacidad de pago de las víctimas.

Ryuk es un Ransomware imperceptible después de la infección inicial. Los atacantes que utilizan Ryuk penetran en las redes a través de vulnerabilidades descubiertas y pueden pasar días o meses antes de propagarse, lo que permite al código malicioso reconocer la red infectada, identificando y apuntando a la red crítica del sistema, para así maximizar el impacto del ataque. Pero también ofrece el potencial de mitigar el ataque antes de que ocurra, si la infección inicial se detecta oportunamente y se logra remediar.

Funcionalidad de Ryuk

Ryuk es una infección de persistencia. Una vez instalado intentará detener ciertos softwares antimalware e instalar la versión de Ryuk dependiendo de la arquitectura del sistema.

Específicamente, después de la ejecución del malware, Ryuk utilizará los comandos predeterminados de Windows taskkill y net stop para deshabilitar más de 180 servicios y más de 40 procesos. Muchos de estos servicios y procesos pertenecen a antivirus, bases de datos, copias de seguridad y software de edición de documentos. Para asegurarse de que el malware se ejecute después de reiniciar, Ryuk utiliza una técnica de persistencia directa, por lo que se escribe a sí mismo en la clave de registro Ejecutar ('reg add / C REG ADD "HKEY_CURRENT_USER \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run" / v "Svchos" / t REG_SZ / d').

Por sí mismo, Ryuk no tiene la habilidad de moverse lateralmente dentro de una red, por lo tanto, la infección de Ryuk depende necesariamente de una infección primaria. Pero si tiene la capacidad de enumerar recursos compartidos de red y encriptar aquellos a los que puede acceder. Lo anterior, junto con el uso de técnicas de recuperación anti-forense del Ransomware (como manipular las shadow copies virtuales) que dificulta la recuperación de copias de seguridad.

Todos los archivos no ejecutables en el sistema son encriptados y renombrados con la extensión “.ryk”. Junto a ello una nota de rescate se coloca en cada carpeta procesada con el nombre “RyukReadMe” (.html o .txt).

Asociación con otros Malware

Ryuk ha sido asociado con otros malware, específicamente con los Troyanos bancarios Emotet y Trickbot.

Emotet es un troyano bancario modular que se detectó por primer vez en 2014, y si bien tiene su propia capacidad, se ha utilizado cada vez más como un agente para facilitar el despliegue de otras amenazas.

Trickbot, por su parte, está presente desde 2016, y emplea técnicas de manipulación del navegador para facilitar el robo de datos con el objetivo de acceder a las distintas cuentas en línea de sus víctimas, que le permiten profundizar los fraudes y generar ingresos a quienes los operan.

De acuerdo a los reportes de la industria a nivel global, cuando ocurre una infección de Ryuk, regularmente se observa un Emotet distribuyendo a Trickbot como parte de una infección en cadena. Enseguida Trickbot implementa herramientas adicionales que permite a quienes operan el malware, incluidos los módulos Mimikatz y PowerShell Empire. Estos facilitan la recolección de credenciales, el monitoreo remoto de la estación de trabajo de la víctima y la realización de movimientos laterales para otras máquinas dentro de una red. Esta infección inicial permite al atacante evaluar si la máquina presenta una oportunidad de ransomware y, de ser así, implementar Ryuk.

Indicadores de Compromiso

Ryuk Ransomware hashes (MD5):

- c0202cf6aeab8437c638533d14563d35
- d348f536e214a47655af387408b4fca5
- 958c594909933d4c82e93c22850194aa
- 86c314bc2dc37ba84f7364acd5108c2b
- 29340643ca2e6677c19e1d3bf351d654
- cb0c1248d3899358a375888bb4e8f3fe

- 1354ac0d5be0c8d03f4e3aba78d2223e

Malware Dropper hashes (MD5):

- 5ac0f050f93f86e69026faea1fbb4450

Recomendaciones


- Bloquear todas las IoC's basadas en en la URL e IP en el firewall, IDS, puertas de enlace web, enrutadores u otros dispositivos perimetrales.
- Actualizar los antivirus y asegurar que su proveedor actual tenga cobertura frente a esta campaña de malware.
- Buscar los signos exitstentes de los IoC's indicados en su entorno y sistemas de correo electrónicos.
- Mantener a salvo los respaldos de los archivos importantes.
- Defender los sistemas de los malware.
- Recordar que pagar el rescate exigido en un caso de Ransomware no garantiza la recuperación de la data.

Fuentes adicionales para la elaboración de este informe:

- <https://www.us-cert.gov/Ransomware> (CISA)
- <https://www.ncsc.gov.uk/news/ryuk-advisory> (UK National Cyber Security Centre)
- <https://exchange.xforce.ibmcloud.com/collection/Ryuk-Ransomware-93beb94af3f3d426b58da0a51e9255ef> (IBM X-Force Exchange)
- <https://research.checkpoint.com/ryuk-ransomware-targeted-campaign-break/> (Check Point Research)

Contactos

 <https://www.csirt.gob.cl>

 + (562) 24863850

 @CSIRTGOB

 <https://www.linkedin.com/company/csirt-gob>