Reporte F-SECURE | Ransomware Wanna Cry

Viernes 12 de Mayo

Los productos F-Secure bloquean el ransomware de WannaCry. Nuestros productos de punto final preventivamente evitan todos los ejemplos in-the-wild del ransomware de WannaCry. El producto de gestión de vulnerabilidades de F-Secure señala las vulnerabilidades utilizadas en el sistema para la corrección.

F-secure ha detectado el ransomware desde su creación, lo que significa que la protección ha estado disponible para todos los clientes finales de F-Secure ya antes del brote. Los productos de punto final F-Secure ofrecen protección contra WannaCrypt en tres capas para asegurar que el ataque puede detenerse en varios puntos durante la cadena de ataque.

1. La función de administración de parches integrada de F-Secure, Software Updater, impide que WannaCrypt explote la vulnerabilidad EnternalBlue implementando automáticamente los parches de seguridad relacionados.

2. La funcionalidad Deepguard de F-Secure proporciona un análisis de comportamiento basado en host y una interceptación de explotación que bloquea WannaCrypt.

3. El firewall de F-Secure evita que WannaCrypt se propague lateralmente en el entorno y encripte archivos.

El administrador de vulnerabilidades de F-Secure, F-Secure Radar, señala el parche de seguridad de Microsoft y el vulnerable puerto 445 para una acción inmediata para los administradores de TI, dándoles tiempo suficiente para solucionar las vulnerabilidades antes del brote.

¿Qué se debe hacer?

1. Asegúrese de que DeepGuard y la protección en tiempo real están activadas en todos los puntos finales corporativos.

2. Identifique los puntos finales sin el parche emitido por Microsoft (4013389) con Software Updater u otra herramienta disponible.

3. Conéctelo inmediatamente con el Software Updater u otras herramientas disponibles.

En caso de que no pueda corregirlo inmediatamente, recomendamos deshabilitar SMBv1 con los pasos documentados en el artículo 2696547 de Microsoft Knowledge Base con el fin de reducir la superficie de ataque

4. Configure el firewall para bloquear correctamente el tráfico

Bloque 445 de entrada a todos los sistemas Windows internos e Internet para evitar que las estaciones de trabajo se infecten

Bloque 455 saliente de servidores para evitar que los servidores se propaguen WannaCrypt dentro del entorno

Como alternativa, puede establecer la política de F-Secure Firewall en su configuración más alta, que tiene reglas predefinidas para bloquear el ataque.

5. Corroborar permisos de escritura generales en la red.

6. Validar que haya un backup en el día o realizar un backup de emergencia en cinta. Cualquier medio de disco puede verse afectado.

7. En cuanto al filtro AntiSpam que tengan instalado, la recomendación es crear una lista de extensiones de archivos java y bloquear todo mail entrante que contenga ese tipo de archivos:

.js

.docm

.jks

.jar

.jse

.vbs

.vbe

.iso

.hta

.wsf

.wncry

En principio la acción podría ser “Etiquetar” en el asunto [posible ransomware] y enviarlo a cuarentena, para tener una idea si están siendo atacados con estos mails. En cuarentena se puede armar un filtro para ver solamente estas etiquetas.

Estos están los nombres de detección asociados a WCry que han reportado hasta ahora:

Gen:Variant.Graftor.374377

Trojan.GenericKD.5054801

Gen:Variant.Graftor.369176

Application:W32/Generic.e889544aff!Online

Gen:Variant.Ransom.WannaCryptor.1

Trojan.Ransom.WannaCryptor.A

Gen:Trojan.Heur.RP.JtW@aePsbmpi

Trojan.GenericKD.5057843

Application:W32/Generic.5ff465afaa!Online

Suspicious:W32/Malware.c5e6c97e27!Online

Application:W32/Generic.47a9ad4125!Online

Trojan.Ransom.WannaCryptor.D

Gen:Trojan.Heur.RP.JtW@aePsbmp

Trojan.GenericKD.5057554

Suspicious:W32/Malware.e889544aff!Online

Suspicious:W32/Malware.5ff465afaa!Online

Suspicious:W32/Malware.51e4307093!Online

Application:W32/Generic.e3712f9d19!Online

Es importante para esta amenaza, que recuerden tener las definiciones actualizadas desde la consola F-secure Policy Manager al día para la distribución a los clientes.

Links con info adicional del fabrincante

Updating virus definition databases

https://help.f-secure.com/product.html?business/policy-manager/12.00/en/concept_30E47A5608AC4C11A9A491F7AD2A9A8F-12.00-en

Trojan.Ransom.WannaCryptor

https://www.f-secure.com/v-descs/trojan_w32_wannacryptor.shtml

WannaCry, the Biggest Ransomware Outbreak Ever

https://safeandsavvy.f-secure.com/2017/05/12/wannacry-may-be-the-biggest-cyber-outbreak-since-conficker/

Tecnología que integramos:

Acerca de NextVision: Desde 1990 integramos Seguridad con soluciones de Tecnología, mediante servicios profesionales especializados, para que la información de nuestros clientes esté siempre protegida y disponible. Desarrollamos proyectos en diferentes mercados – como Banca y Finanzas, telecomunicaciones, Oil & Gas y Servicios, entre otros – y para diversas organizaciones de gobierno, tanto en Argentina como en América Latina y Europa. Para más información, ingresar a www.nextvision.com