Asesoramiento para la Remediación de WannaCry

Cómo detectar y remediar WannaCry con el Servicio de Control de Vulnerabilidades (SCV)

UN BROTE GLOBAL

WannaCry (también conocido como WanaCrypt, WanaCryptor 2.0 y Wanna Decryptor) es una nueva variante de ransomware que explota un grupo de vulnerabilidades de Microsoft Windows, conocidas colectivamente como MS17-010. Se identifican en la base de datos de vulnerabilidades del SCV mediante los siguientes códigos: CVE-2017-0143, CVE- 2017-0144, CVE-2017-0146, CVE-2017-0146, CVE-2017-0147 y CVE-2017-0148.

WannaCry se propaga rápidamente a través de las redes utilizando un exploit llamado **EternalBlue** como mecanismo de distribución. EternalBlue apunta a la vulnerabilidad MS17-010 y utiliza un componente de gusano para propagarse. En la mayoría de los casos, un ransomware debe descargarse activamente en cada máquina a través de una vulnerabilidad del navegador o un correo electrónico de suplantación. Sin embargo, WannaCry solo necesita ser descargado en una máquina, tras lo cual continua propagándose por la red a través de Windows SMB (Server Message Block).

Microsoft lanzó un parche para sistemas soportados afectados por MS17-010 el 14 de marzo de 2017. **ANADAT** a través de nuestra plataforma basada en la solución de **SkyBox Security** publicó la vulnerabilidad en la base de datos 15 de marzo de 2017.

Después de evaluar la inteligencia de amenazas en tiempo real por el Laboratorio de Investigación, las vulnerabilidades MS17-010 fueron marcadas como explotables "in the wild" el 18 de abril de 2017 en el Centro de Priorización del Servicio de Control de Vulnerabilidades de SkyBox.

Algunos sistemas afectados por el MS17-010 ya no están soportados por Microsoft, y no había parches disponibles para Microsoft Windows XP, Windows Server 2003 y Windows 8 en la actualización de 14 de marzo de Microsoft. Después del brote de WannaCry, sin embargo, Microsoft publicó parches para estos sistemas el 13 de mayo de 2017.

RECOMENDACIONES

PROTEJA Y RESPONDA: Servicio de Control de Vulnerabilidades

Los servicios de **ANADAT** para la gestión y control de vulnerabilidades y simulación de amenezas, pueden ayudar en la corrección de vulnerabilidades y reglas de acceso explotadas por la variante de Ransomware de WannaCry. También pueden ayudar a prevenir ataques similares en el futuro.

GESTIÓN DE VULNERABILIDADES Y AMENAZAS

Utilice el Servicio de Control de Vulnerabilidades para identificar y remediar las vulnerabilidades explotadas por WannaCry.

Paso 1: Descubrimiento

El Servicio de Control de Vulnerabilidades puede identificar todos los dispositivos que contienen las vulnerabilidades MS17-010. Esta identificación se puede realizar en cuestión de minutos mediante la función de detección de vulnerabilidades.

El control de la vulnerabilidad también puede utilizarse para realizar un seguimiento rápido de los esfuerzos de remediación ejecutándolo cada pocas horas (algo imposible mediante exploración tradicional).

Paso 2: Priorización

Nuestro servicio de control y gestión de las vulnerabilidades identifica las vulnerabilidades MS17-010 como explotadas **"in the wild"** y las etiqueta con una gravedad crítica en el Centro de Priorización.

La plataforma también identifica los puntos calientes de la infraestructura con alta densidad de la vulnerabilidad en las unidades de la organización y en todas las zonas geográficas, marcándolos para su inmediata selección y corrección.

La simulación de ataques de la plataforma identifica la exposición frente a ataques de terceros y otras conexiones externas, pues es posible que desee cerrar estas conexiones para protegerse contra futuras infecciones.

Paso 3: Remediación

Aplique parches y / o utilice firmas IPS, reglas de acceso y segmentación de red para bloquear rutas de ataque.

Utilice el Centro de Remediación para realizar un seguimiento del estado de remediación de MS17-010, asegurándose que se llevaron a cabo todos los procedimientos adecuados y no se omitieron dispositivos.

Recomendamos adoptar un enfoque de utilización del Servicio de Control de Vulnerabilidades para monitorizar continuamente nuevas vulnerabilidades, identificar cambios en la exposición de activos y la aparición de nuevas amenazas que circulan **"in the wild".**

GESTIÓN DE FIREWALLS Y POLÍTICAS DE SEGURIDAD

Utilice los módulos "Firewall Assurance, Network Assurance y Change Manager" para cambiar las reglas del firewall o de dispositivos de red y bloquear la propagación del exploit.

- Identificar todas las rutas y reglas de firewall que utilizan los servicios infectados — Server Message Block (SMB): 135, 139,445
- Revisar y considerar sus requerimientos como parte de la segmentación de la red para minimizar la propagación de la infección
- Crear solicitudes de cambio para eliminar estas reglas y prevenir más infecciones
- Revisar la topología de la red, las conexiones de terceros y las rutas de acceso
- Asegúrese de que estas rutas bloqueen cualquier ruta de ataque potencial

RECURSOS ADICIONALES

La página de Threat-Centric Vulnerability Management (TCMV) de Skybox, tecnología sobre la que se basa la plataforma de **ANADAT**, tiene gran cantidad de información, incluido un resumen de la solución TCVM, informe técnico, informe de Gartner y mucho más.

PREVENIR UN ATAQUE SIMILAR EN EL FUTURO

- Abordar los problemas subyacentes relacionados con la mala "ciber-higiene" de inmediato
- Llevar a cabo una evaluación exhaustiva del riesgo de todas las vulnerabilidades en su red, incluyendo la nube y el entorno virtual, usando el Servicio de Control de Vulnerabilidades.
- Priorizar la remediación de vulnerabilidades por amenazas "inminentes" y "potenciales" usando Vulnerability Control; desarrollar un plan para remediar inmediatamente las amenazas inminentes y rastrearlo hasta su finalización; ocuparse de las amenazas potenciales con el tiempo
- Cambie su enfoque de la simple gestión de vulnerabilidades a la gestión de vulnerabilidades centrada en amenazas (consulte Skybox TCVM)
- Identificar y auditar el perímetro de su red para que la entrada / salida sea identificada apropiadamente; comprender el alcance del acceso que todos los terceros tienen en su red mediante Network Assurance y Firewall Assurance
- Audite la infraestructura de red y firewall con regularidad para encontrar las configuraciones erróneas utilizando Firewall Assurance y Network Assurance
- Generar la evaluación de cumplimiento y riesgos en los procesos de cambio en firewalls mediante Change Manager
- Desarrollar políticas de acceso organizacional y estándares de configuración adecuados al objetivo, utilizando Firewall Assurance y Network Assurance
- Construir y mantener una comprensión detallada de los activos de su red, incluidas las redes en la nube y las redes virtuales, alineadas con la criticidad empresarial mediante el Servicio de Control de Vulnerabilidades.

Si tiene preguntas adicionales o desea una demostración de la plataforma para guiarlo a través de cualquiera de los pasos que hemos recomendado aquí, puede ponerse en contacto con nosotros a través del correo electrónico Marketing@anadat.es o número de teléfono 902 19 60 47

Sobre el Servicio de Control de Vulnerabilidades de ANADAT Consulting

El Servicio de Control de Vulnerabilidades de **ANADAT** arma a los responsables de seguridad con el conjunto más amplio de soluciones para las operaciones de seguridad, el análisis y la generación de informes. Se integra con más de 100 tecnologías y utiliza un modelado de red, el análisis del vector de ataque y la evaluación de vulnerabilidades multifactorial para dar una visibilidad sin precedentes de la superficie de ataque y los indicadores de exposición (IOEs). Esto proporciona a los responsables de seguridad la visión necesaria para una gestión eficaz de las vulnerabilidades centrada en las amenazas y la gestión automatizada de firewalls y de políticas de seguridad a través de redes físicas, virtuales y en la nube.