CIBERATAQUES PRODUCIDOS A ESCALA MUNDIAL

En relación con los ataques informáticos masivos contra diferentes entornos productivos, iniciados el pasado mayo de 2017, mediante la utilización del ramsomware WannaCry combinado con la vulnerabilidad EternalBlu, se informa de lo siguiente:

SOBRE EL ATAQUE

A última hora de la mañana del 12 de mayo de 2017 y a través de una alerta de la Compañía Telefónica, se detectó un nuevo ransomware (desde 2015 se han identificado más de 50 variantes) que se propagaba como un gusano, aprovechando las vulnerabilidades del protocolo SMB de Windows (que permite la compartición de archivos entre nodos de una red), lo que le confería excepcionales cualidades de propagación e infección. En esta ocasión se trata del ransomware, conocido como WannaCrypt (en su versión 2.0), y que parece haber afectado a los equipos que no han aplicado el parche para estas vulnerabilidades (parche MS17-10 publicado por Microsoft el pasado 14 de marzo).

Una amenaza de ransomware normalmente no se propaga tan rápidamente, suelen aprovechar la ingeniería social o los correos electrónicos como vector de ataque principal, dependiendo de que los usuarios descarguen y ejecuten. Sin embargo este ransomware incorpora el código de explotación públicamente disponible denominado EternalBlue, que permite explotar y atacar los sistemas Windows 7 y Windows Server 2008 y anteriores (al no existir parche previo, pues la compañía Microsoft ha publicado uno de urgencia el día 13 de mayo), así como los sistemas Windows 10 no previamente parcheados con la actualización MS17-010.

Su novedoso mecanismo de propagación, que aprovecha las vulnerabilidades que se hicieron públicas a través de Wikileaks a mediados del pasado mes de marzo, han armado a este ransomware regular con funcionalidades semejantes a gusanos, creando un poderoso vector de ataque sobre las máquinas (nodos) que aún están sin parchear e interconectadas en un segmento de Red de Área Local LAN.

Aunque aún no se ha hecho pública la evidencia del vector de entrada en las organizaciones afectadas, todo parece indicar que existen dos posibles escenarios, a su vez complementarios, para esta familia de ransomware:

- Llegada a través de mensajes de correo electrónico de ingeniería social diseñados para engañar a los usuarios para que ejecuten el malware y de este modo se active la funcionalidad de difusión y la explotación de SMB, dando origen a lo que sería el “huésped cero” en una LAN / WAM (Intranet) determinada.
- La infección a través del protocolo SMB de cuantos nodos (ordenadores, servidores, impresoras, etc) estén presentes en la LAN / WAN y sean vulnerables por no estar parcheados.

El CCN-CERT ha publicado una herramienta para evitar esta infección (NoMoreCry2000-v0.3) pero que no suple al parche de la Compañía Microsoft, sino que lo complementa.

El lunes 15 de mayo, se produjo la pronosticada y temida reactivación del ciberataque con, al menos, tres variantes (mutaciones) del ramsomware original, con diferentes niveles de impacto tanto a nivel nacional como internacional.

IMPACTO EN ESPAÑA

El Instituto Nacional de Ciberseguridad (Incibe), informó el 15 de mayo que España ocupaba la posición 18 del listado de países afectados por las distintas variaciones del virus WannaCrypt, con menos de diez empresas afectadas (operadores estratégicos) y 1.200 infecciones conocidas. No habiéndose producido nuevas infecciones durante el lunes 15, a primera hora del día 16 se tuvo conocimiento que varias PYMES se estaban viendo afectadas, por lo que se puede hablar de un rebrote a nivel nacional (aún es pronto para conocer la magnitud real de éste).

IMPACTO EN EL MUNDO

Se estiman en más de 300.000 las infecciones en todo el Mundo desde el inicio del ataque el pasado viernes, por las diferentes variantes de este virus, en un total de 179 países (fuente Europol). Los más afectados son China, Rusia, Estados Unidos y Reino Unido, donde se destaca que habría afectado a sistemas o redes que podrían haber impactado en servicios esenciales de la salud, transporte o sistema financiero, si bien estas infraestructuras no eran el objetivo principal del ciberataque.
La segunda oleada de infecciones se ha cebado mayoritariamente con los países asiáticos, como Japón, con 600 empresas y cerca de 2.000 ordenadores comprometidos, y especialmente China, que ya ha confirmado que cientos de miles de ordenadores en 29.372 instituciones se están viendo afectados, aunque no se dispone de cifras exactas.

MEDIDAS PREVENTIVAS

En la siguiente lista se resumen las principales medidas que se han de adoptar, en orden de prioridad, para prevenir, detectar y/o mitigar parcialmente la acción de un ransomware:

- Mantener copias de seguridad periódicas (backups) de todos los datos importantes. Es necesario mantener dichas copias de seguridad aisladas y sin conectividad con otros sistemas, evitando así el acceso desde equipos infectados.
- Mantener el sistema actualizado con los últimos parches de seguridad, tanto para el sistema operativo como para el software que hubiere instalado.
- Mantener una primera línea de defensa con las últimas firmas de código dañino (antivirus), además de disponer de una correcta configuración de firewall a nivel de aplicación.
- Disponer de sistemas antispam a nivel de correo electrónico, y establecer un nivel de filtrado alto, para así reducir las posibilidades de infección a través de campañas masivas de ransomware por mail.
- Establecer políticas de seguridad en el sistema para impedir la ejecución de ficheros desde directorios comúnmente utilizados por el ransomware (App Data, Local App Data, etc). Herramientas como AppLocker, Cryptoprevent o CryptoLocker Prevention Kit, permiten crear fácilmente dichas políticas.
- Bloquear el tráfico relacionado con dominios y servidores C2 mediante un IDS/IPS, evitando así la comunicación entre el código dañino y el servidor de mando y control.
- Establecer una defensa en profundidad empleando herramientas como EMET.
- No utilizar cuentas con privilegios de administrador.
- Mantener listas de control de acceso para las unidades mapeadas en red. En caso de infección el cifrado se producirá en todas las unidades de red mapeadas en el equipo víctima. Restringiendo los privilegios de escritura en red se mitigará parcialmente el impacto.
- Se recomienda el empleo de bloqueadores de JavaScript para el navegador, como por ejemplo “Privacy Manager”.
- Adicionalmente, se recomienda la instalación de la herramienta “Anti-Ransom”, que tratará de bloquear el proceso de cifrado de un ransomware.
- Finalmente, el empleo de máquinas virtuales evitará en un alto porcentaje los casos de infección por ransomware.

Madrid, Mayo/2017