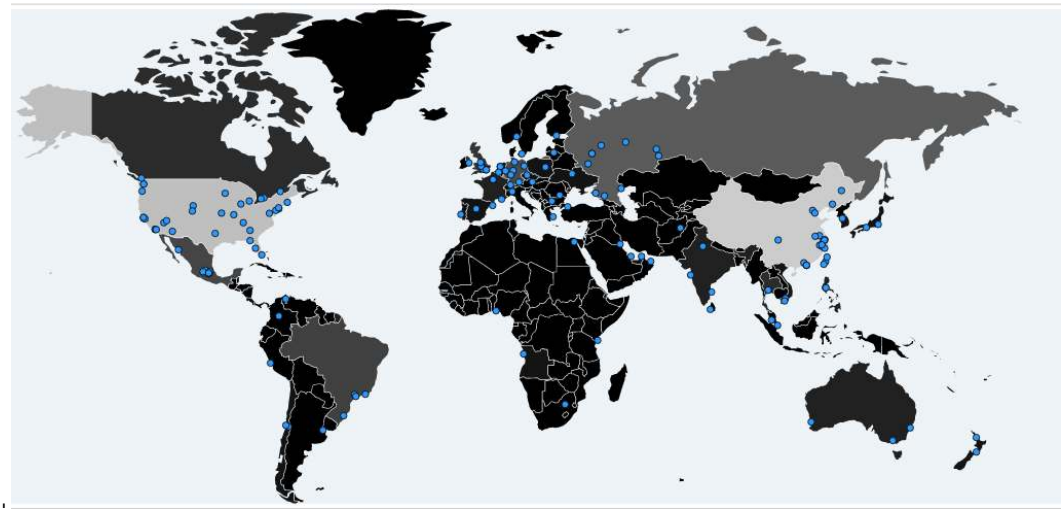
proactive
Information security.

Ayudamos a Proteger sus Activos de Información

ProActive News Vol.2

¿Qué pasó, un ciberataque a nivel mundial?

Como anunciamos hace unas semanas en nuestra primera edición de noticias, se debía tener cuidado con los exploits liberados de la NSA por ***The Shadow Brokers*** ya que estos permitían acceder a equipos que no posean la actualización **MS17-010** y tomar control del mismo. Entonces, qué pasó? Un grupo de personas mal intencionadas decidió hacer uso del exploit y transformarlo en un *ransomware* llamado ***Wannacry*** que cifra la información de la PC, buscando también expandirse por la red, explotar y cifrar nuevas PCs que **NO** posean la actualización MS17-010 instalada. A continuación te mostramos el mapa de los países más afectados:



https://intel.malwaretech.com/botnet/wcrypt

¿Qué sistemas se vieron afectados por *Wannacry*?

El *ransomware* fue programado para afectar principalmente a los siguientes sistemas:

- Windows 7
- Windows 2008 Server.

Una vez que la PC era infectada, aparecía la siguiente pantalla:

Maquina infectada

¿Cómo puede ocurrir la infección?

Pues, de diferentes maneras: por e-mail, un *pendrive* dejado en algún lugar de tu empresa, un atacante interno, en fin, existen múltiples formas de producir la infección de una PC.

¿Se puede descifrar la infección?

Depende... cada caso es particular, no existe hasta el momento un herramienta capaz de descifrar cualquier PC infectada por el *ransomware wannacry*, hay herramientas de recuperación de la información pero son para escenarios particulares, un escenario por ejemplo, es cuando la PC no se apagó.

¿Cómo se defiende mi Organización?

Lo primero que recomendamos es tener al personal capacitado. Si tu personal esta consiente de los riesgos que puede tener para tu empresa abrir un archivo que viene de un origen desconocido, será más difícil que el *malware* entre por ese medio.

Como segunda medida, estar al día con todas las actualizaciones de Microsoft ayuda bastante para evitar la propagación del malware, si los equipos están actualizados no podrá expandirse.

Desde nuestro punto de vista, la copia de respaldo frecuente (*backup*) de la información es fundamental, y los periodos dependen del tipo de información. Entre más crítica sea la información, se hace una copia con más frecuencia.

Tener Antivirus, IDS/IPS, SÍ, son importantes, agregan una capa de seguridad, pero es una medida que estará siempre en una capa inferior a la de los ataques. Tener estas medidas no evita las infecciones.

Con objeto de mantenerlo actualizado y protegido, quedamos a vuestra disposición para asesorarlo en cuanto a la detección de vulnerabilidades en su plataforma que puedan ser explotadas por los recientes exploits filtrados.

Obtenga mayor información sobre nuestros servicios y productos, póngase en contacto con nosotros:

Web: www.proactive.consulting

Mail: contacto@proactive.consulting

Tel: +595 (981) 478-921

Twitter: @ProActive_py