Alerta de ransomware: Wannacry

Desde hace tiempo venimos escuchando de ransomware, sin embargo las organizaciones no habían prestado la suficiente atención al tema pues no había ocurrido un episodio que afectara de forma masiva a personas y empresas alrededor del mundo o casos de empresas de amplio reconocimiento que fueran el objetivo de los cibercriminales.

Sin embargo, esta situación cambió con las noticias del pasado viernes 12 de mayo cuando mas de 200.000 ataques en 150 países fueron perpetrados, y en la cual empresas como Telefónica y Gas Natural en España, el Servicio Nacional de Sanidad (NHS) y hospitales en el Reino Unido, el fabricante francés de automóviles Renault, la empresa de correos estadounidense FedEx, el ministerio del Interior ruso y el operador de ferrocarriles alemán Deutsche Bahn y el Instituto Nacional de Salud y el Ministerio de Justicia en Colombia, fueron victimas.

El mismo viernes un investigador encontró que el malware realizaba una validación con un dominio en Internet y al registrarlo quedó temporalmente neutralizado. No obstante, investigadores de China confirmaron lo que denominaron la versión 2.0, la cual no posee esta debilidad y ha continuado con la infección masiva.

¿POR QUÉ ESTE ATAQUE ES LETAL?

Lo que hace particular este ataque es que utiliza la variante de ransomware conocida como **"WannaCry",** la cual se vale de una vulnerabilidad de varios sistemas operativos Microsoft Windows para propagarse (ver boletín de seguridad). Según han informado varios analistas la herramienta para explotarla fue desarrollada por la agencia de seguridad NSA de los E.E.U.U y sería parte del robo perpetrado por el grupo de hackers conocido como "Shadow Brokers".

El malware aprovecha una falencia en el protocolo SMB de Windows, al recurso $IPC, sobre el cual es posible la ejecución de código remoto, lo que permite una rápida propagación en las organizaciones, incluso sin necesidad de la accion de los usuarios. Más información en los siguientes enlaces:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0145
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0146
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0147
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0148

Las actualizaciones para "parchar" esta vulnerabilidad fueron liberadas por Microsoft desde el pasado 14 de Marzo de 2017. Sin embargo, una gran cantidad de empresas y personas no las habían corrido en sus sistemas y aun se encontraban vulnerables. Muchos de estos corresponden a sistemas operativos que salieron de soporte como Windows XP o Windows Server 2003 o que alojan aplicaciones de misión crítica y que no habian podido ser reiniciados para completar el proceso. Debido a la gravedad de lo que esta sucediendo y en un hecho sin precedentes Microsoft libero actualizaciones de seguridad de emergencia para estos sistemas legacy. Puede encontrar los links de descarga de los mismos en el siguiente enlace:

https://social.technet.microsoft.com/wiki/contents/articles/37915.you-dont-need-to-cry.aspx

MEDIDAS DE PROTECCIÓN

- **Aplique las actualizaciones en sus sistemas operativos** para asegurar que se encuentran protegidos ante la vulnerabilidad descrita.
- Aplique las políticas y parches que fabricantes de seguridad se encuentran publicando en este momento. TrendMicro ha publicado las siguientes:

- OSCE XGen - Patrón 13.399.00 y 17264.014.00
- Deep Security & Vulnerability Protection- Patrón DSRU-ID 17-016
- Deep Discovey Inspector - Rule ID 2383: CVE-2017-0144 - RCE - SMB (Request)
- Tipping Point - filters: 27433, 27711, 27928
- High-Fidelity Machine Learning detecta SIN necesidad de patrón
- Deep Discovery Custom Sandbox detecta SIN necesidad de patrón

Para mayor informacion visite este enlace:

- **Actualice su herramienta de antimalware a la última versión** y verifique que los agentes se encuentren en modo online. Después de actualizar los patrones, **realice una exploración manual programada en sus dispositivos.**

- **Asegúrese de que las inspecciones de AV e IPS de Fortinet, así como los motores de filtrado web estén activados** para evitar que se descargue el malware y para asegurar que el filtrado web está bloqueando las comunicaciones a los servidores de comando y control.

- IPS signature: SMB.Server.SMB1.Trans2.Secondary.Handling.Code.Execution
- AntiVirus signatures:

* W32/Filecoder_WannaCryptor.B!tr
* W32/WannaCryptor.B!tr
* W32/Generic.AC.3EE509!tr
* W32/GenKryptik.1C25!tr

- **Deshabilitar la versión SMBv1** del protocolo SMB, hacer uso de las versiones posteriores.
- **Haga restricción de las conexiones a nivel Firewall sobre el protocolo SMB** (puertos: 135 UDP, 137 UDP, 138 UDP, 139 UDP, 445 UDP/TCP) para evitar que la vulnerabilidad MS17-010 sea explotada de forma externa. Bloquear todas las conexiones que vengan desde Internet hacia los puertos mencionados anteriormente. Si requiere hacer uso de este servicio, se recomienda que se realice a través de una conexión segura (VPN).
- De ser posible, **bloquee la transferencia de archivos a través de correo electrónico**, especialmente aquellos con extensiones .exe, .jar, .bin, .msi.
- Generalmente los dominios en los que se alojan los C&C, y donde se encuentran los servidores de descarga del malware, se ocultan en la red tor bajo el dominio tro2web o dominios .onion. **Bloquee el acceso a estos dominios, mediante dispositivos de filtrado WEB y/o AntiSpam** creando reglas que analicen el asunto y cuerpo de mail en busca de dominios maliciosos.
- **Asegúrese de contar con copias de seguridad de su información** para limitar el posible impacto causado por la pérdida de datos o sistemas y ayudar en el proceso de recuperación.
- **Prohiba la creación de archivos con doble extensión**, ya que se ha podido identificar que el malware en el proceso de cifrado, genera archivos con doble extensión (Ejem: archivo.doc.wannacry).
- **Implemente mecanismos de detección** de amenazas desconocidas (ransomware, APT, etc).
- **Comunique a los usuarios** sobre la amenaza, su impacto y medidas de protección de los dispositivos de sus hogares y la organización. Algunos elementos infografías y videos que hemos desarrollado pueden ser de ayuda.
- **Alerte a todos los usuarios** de no ejecutar archivos sospechosos o con extensiones peligrosas (exe, jar, bin, msi, etc).

[Actualización] EternalRocks, el sucesor de Wannacry

En los últimos días han estado apareciendo nuevas amenazas relacionadas con Wannacry. Algunas han sido consideradas potencialmente más peligrosas. Este es el caso de un nuevo malware conocido como EternalRocks el cual explota 7 vulnerabilidades que fueron filtradas de la NSA y que utiliza como medio de propagación: EternalBlue, EternalChampion, EternalRomance, EternalSynergy, SMBTouch, ArchiTouch y DoublePulsar.

Hasta el momento se sabe que debido al alto número de vulnerabilidades que puede explotar la potencial capacidad de propagación de EternalRocks es significativamente más alta (WannaCry ha infectado más de 300.000 máquinas en el mundo haciendo uso de solo una vulnerabilidad). Hasta el momento no se sabe cuales son las actividades maliciosas que ejecuta; sin embargo hay una alta posibilidad de generación de campañas de espionaje, robos de información o creación de redes zombie.