Departamento de Seguridad Informática MINSAP

Abril 2017

Volumen 1, nº 1

Boletín de Seguridad Informática

Contenido:

Puntos de interés especial:

-Hay una serie masiva de ciberataques en todo el mundo en este momento y el malware que se ha filtrado desarrollado por la NSA parece ser la culpa. Ransomware, un software que encripta los datos de la víctima y exige un rescate para desbloquearlo.

-Para Microsoft, los recientes escándalos sobre la CIA y la NSA están estrechamente ligados con este problema de relevancia internacional.

-Los Estados Unidos han publicado sus propias reglas para que cualquiera pueda utilizarlas en sus servicios de inteligencia frente amenazas.

Un ciberataque global está usando una vulnerabilidad de la NSA para derribar hospitales y compañías de telecomunicaciones

Hay una serie masiva de ciberataques en todo el mundo en este momento – y el malware que se ha filtrado desarrollado por la NSA parece ser la culpa. Ransomware, un software que encripta los datos de la víctima y exige un rescate para desbloquearlo, se ha extendido a por lo menos 74 países, desde Inglaterra a Japón. Entre las organizaciones afectadas están el gigante español de las telecomunicaciones Telefónica (que dijo hoy a los empleados que dejen de trabajar y apaguen sus computadoras, según el periódico español El Mundo) y el Servicio Nacional de Salud (NHS) del Reino Unido.

Al menos 15 organizaciones del NHS en todo el Reino Unido se han visto afectadas, causando caos total. Los hospitales han sido cerrados y las operaciones canceladas con poca antelación, y el personal médico ha recurrido a la pluma y el papel para trabajar. La firma de logística FedEx también se ha visto afectada, según la BBC.

Tanto NHS como Telefónica confirmaron los ataques. Ambos dijeron que habían sido golpeados por las versiones del programa de ransomware "WannaCry" – software malicioso que cifra la información en un dispositivo, y luego exige un rescate para devolverlo. Según los informes de los usuarios en Twitter, el ransomware pide a los usuarios que paguen $300 en Bitcoin (mas de US$500,000). La razón de la propagación virulenta del malware parece ser el uso de una vulnerabilidad del software de Windows desarrollado por la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés), una agencia espía estadounidense. La vulnerabilidad se filtró hace meses y se

corrigió por Microsoft, pero los afectados parecen no haber actualizado su software para instalar la corrección. Según The New York Times, el malware se ha detectado en al menos 12 países.

Alrededor del 85% de las computadoras de Telefónica se han visto afectadas. Portugal Telecom (PT) también se ha visto afectada, aunque una portavoz no dijo si se trataba de un ataque de WannaCry. La compañía dijo que sus sistemas no se habían visto afectados, según Reuters.

El equipo nacional de respuesta informática de España, CN-CERT, emitió un aviso sobre los ataques.El viernes, CCN-CERT, el equipo español de respuesta a emergencias informáticas, publicó un comunicado vinculado a los ataques de ransomware.“El ransomware, una versión de WannaCry, infecta la máquina cifrando todos sus archivos y, usando una vulnerabilidad de ejecución remota de comandos a través de SMB, se distribuye a otras máquinas Windows en la misma red”, escribió la organización. También apuntan a un parche de Microsoft.

Microsoft culpa a los gobiernos del ‘hackeo’ internacional

Microsoft no tenía culpa, sencillamente, porque lanzaron una actualización para cerrar la **vulnerabilidad aprovechada por WannaCry**. Es más, incluso actualizaron Windows XP. Y a las empresas *‘les pilló el toro’* no por desinterés en los **parches de seguridad**, sino porque hay aplicaciones propias que requieren de cierta cautela al modificar cualquier aspecto relativo al software. Para Microsoft, los recientes **escándalos sobre la CIA y la NSA** están estrechamente ligados con este problema de relevancia internacional.

El **ransomware** ha afectado desde el pasado viernes a **empresas y organizaciones de todo el mundo**. Pero lo más curioso no está en cómo ha acabado la historia –*que aún no ha concluido, en realidad*- sino en **cómo empezó todo**. Y la cuestión está en que la vulnerabilidad aprovechada fue descubierta por **Equation Group**, un grupo relacionado con la **Agencia de Seguridad Nacional** de los Estados Unidos, y catalogada como uno de los grupos informáticos más sofisticados del mundo. Pero esta vulnerabilidad, que se mantenía ‘en secreto’, **se filtró** por parte de **Shadow Brokers.**

La NSA conocía la vulnerabilidad y Microsoft culpa a los gobiernos del problema.

En un comunicado, Microsoft ha recordado la importancia de la **relación entre gobiernos y empresas** privadas para cuestiones de este tipo. Una **vulnerabilidad** es como un ‘arma’, según la compañía de Redmond, y debe tratarse como tal. Se ha demostrado que tienen razón los de Microsoft, en tanto que **si la NSA hubiese informado a Microsoft**, el problema se podría haber abordado **de otra manera**. Sin embargo, tal y como han sucedido las cosas, el parche llegó más tarde de lo deseable, y finalmente el ransomware ha tenido un **impacto a nivel mundial.**

En esta carta, Microsoft ha aprovechado para recordar las **filtraciones de la CIA** por parte de WikiLeaks.

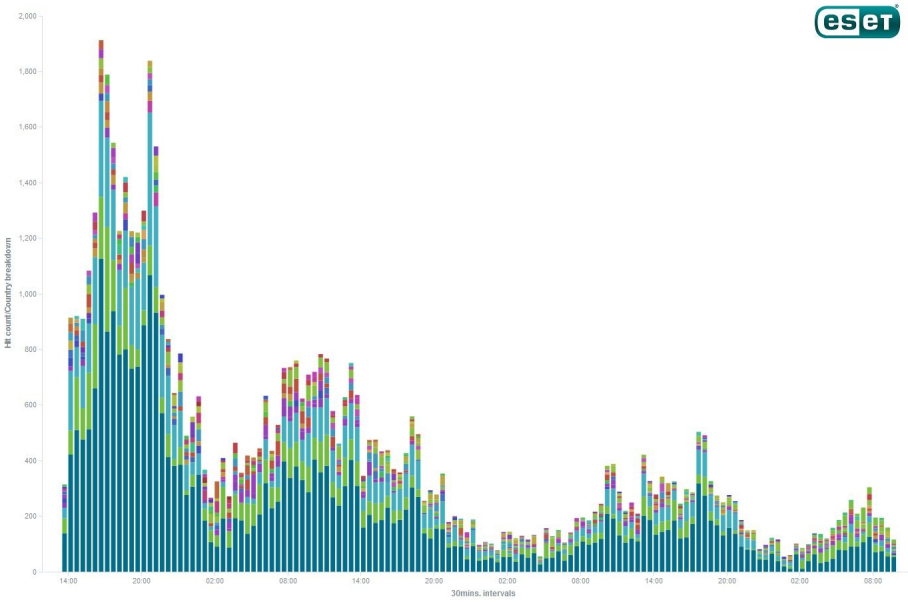
Y en este sentido, la compañía de Redmond ha atizado con dureza al gobierno de los Estados Unidos por **no colaborar** con las empresas privadas dedicadas al mundo de la informática para **proteger a los ciudadanos y usuarios de Internet**. Este texto lo han titulado ***'lecciones del ciberataque'***, y desde Microsoft se han mostrado comprometidos a **empujar la colaboración** entre empresas y gobiernos de todo el mundo para **evitar que manejen y aprovechen las vulnerabilidades** en contra de los ciudadanos.

EVOLUCIÓN DE WANNACRYPTOR Y ANÁLISIS DE LAS CONSECUENCIAS DEL ATAQUE

Tras un fin de semana en el que analistas de malware, investigadores, administradores de sistemas, técnicos de soporte y otras profesiones relacionadas con la ciberseguridad hemos descansado poco, toca hacer balance de la situación y ver que es lo que puede suceder a partir de ahora, ya empezada una nueva semana y con la gente volviendo a sus puestos de trabajo.

Nuevas variantes

Los datos recopilados en las últimas horas nos indican cosas muy interesantes, como por ejemplo el intento de desarrollar nuevas variantes sin el interruptor de apagado que se activaba tras contactar con la dirección URL introducida en el código del malware. Sin embargo, hasta el momento, ninguna de estas variantes sin ese "Kill Switch" son plenamente funcionales, aunque puede ser cuestión de tiempo que los delincuentes lo corrijan (si es que quieren seguir desarrollando este ransomware y no cambiar de malware). Con los datos de los que disponemos en nuestro laboratorio y gracias a las reglas Yara creadas en nuestro servicio ESET Threat Intelligence hemos podido ir cuantificando las nuevas variantes que han ido apareciendo. También algunos investigadores u organismos públicos como el CERT de los Estados Unidos han publicado sus propias reglas para que cualquiera pueda utilizarlas en sus servicios de inteligencia frente amenazas. Gracias a estos datos recopilados y a la ayuda de nuestro compañero Jiri Kropac de los laboratorios de ESET en la República Checa hemos podido observar de forma gráfica la evolución de WannaCryptor desde su aparición el pasado viernes 12 de mayo hasta esta misma mañana.



Como observamos, la mayor parte de detecciones se realizó durante el viernes y el sábado. Algo comprensible debido a la elevada velocidad de propagación debido a las capacidades de gusano de WannaCryptor. El descenso durante el fin de semana se debe principalmente a que la mayoría de empresas afectadas estuvieron cerradas durante esos días y que la activación del Interruptor de apagado gracias al registro de un dominio por parte de dos investigadores británicos consiguió frenar el proceso de propagación. En lo que respecta a número de variantes detectadas hasta el momento de escribir estas líneas, en ESET detectamos cuatro variantes principales de nombre Win32/ Filecoder.WannaCryptor y sus variantes A,B,C y D, junto con sus múltiples subvariantes.

En relación a los países más afectados de nuestro entorno, si nos centramos en la región de EMEA (Europa, África y Oriente Medio) observamos como Rusia es claramente el país más afectado, al menos por una de las variantes más propagadas. España estaría en la parte media de la tabla con unas 170 empresas afectadas por esa variante de WannaCrypt a día de hoy (a las que habría que sumar el resto).**Aparecen los imitadores**

En rio revuelto, ganancia de pescadores, reza el refranero español y esta situación no es una excepción. Viendo el éxito de WannCryptor, no son pocos los delincuentes que se han puesto a propagar otras variantes de ransomware, aunque la gran mayoría de ellas siguen utilizando el método tradicional del correo electrónico con adjunto malicioso.Así pues, y como muy bien resumen en el blog Bleeping Computer, durante los últimos días se ha observado la propagación o el desarrollo de otras variantes de ransomware que se aprovechan del tirón de WannaCryptor y que responden a nombres como Wanna Crypt v2.5, WannaCrypt 4.0, DarkoderCryptor o una utilidad para personalizar la pantalla de bloqueo y las instrucciones de pago y descifrado conocida como Aron WanaCrypt0r 2.0 Generator v1.0.

Lo cierto es que el impacto de Wannacryptor se ha podido ver en todo el mundo y, durante todo el fin de semana se han ido compartiendo fotografías de sistemas afectados como ordenadores, cajeros automáticos, paneles informativos o incluso paneles luminosos colocados en plena calle como el que vemos a continuación:

Principales consecuencias

Además de habernos tenido ocupados a muchos especialistas en seguridad informática, administradores de sistemas y otras muchas personas, la llegada del lunes ha supuesto una prueba de fuego para muchas empresas. Algunos de los incidentes más madrugadores se han producido en la zona de Asia, donde la empresa japonesa Hitachi también se ha visto afectada por estas variantes de WannaCryptor.En lo que respecta a España, la situación ha estado bastante controlada, con algún incidente aislado. Esto no significa, ni mucho menos, que la amenaza haya desaparecido puesto que el principal problema no se encuentra en el ransomware propiamente dicho, si no en la funcionalidad de gusano que se le ha incorporado y que puede ser portada a otro tipo de malware fácilmente.

No es difícil pensar en un malware que se propague de la misma forma y que, en lugar de alertar enseguida a sus víctimas mostrando una pantalla con un mensaje alarmante, permanezca oculto y se dedique a robar información de forma sigilosa o a destruirla en una fecha programada por los atacantes. Algunos expertos como Sergio de los Santos apuntan a que esta vulnerabilidad no sería la única que se podría utilizar para aportar funcionalidades de gusano a casi cualquier malware y mencionan a la solucionada recientemente por Microsoft y que afectaba a Windows Defender.

Lo que se ha comprobado casi a ciencia cierta es que estas variantes de WannaCryptor no utilizaron ningún correo con fichero adjunto para propagarse inicialmente tal y como viene siendo habitual y que, una vez dentro de una red corporativa, se propagaban rápidamente de un equipo vulnerable a otro aprovechando el exploit EternalBlue. En el siguiente vídeo realizado por el investigador Hacker Fantastic se puede ver claramente: Respecto al dinero obtenido por los delincuentes en las tres carteras de bitcoin que pusieron a disposición de los afectados por el ransomware para realizar el pago de los rescates, estas no han reunido una cantidad significativa a pesar de haber conseguido infectar más de 200.000 sistemas y, en el momento de escribir estas líneas apenas habían recopilado poco más de 50.000 dólares.

Conclusión

Todo apunta a que la situación está más o menos controlada (en algunas regiones mejor que en otras) y que, salvo la aparición de alguna nueva variante con cambios significativos las infecciones tenderán a remitir. No obstante, este incidente debe servir como

una importante llamada de atención para mejorar muchos aspectos relacionadas con la ciberseguridad en las empresas.

La revisión y aplicación de actualizaciones periódicas de seguridad (como la MS17-010 que evita que los sistemas sean vulnerables) es algo que se debe tener en cuenta, aun sabiendo que existen muchos tipos de empresas y no siempre es factible instalarlas sin que pase antes un largo periodo de tiempo revisando que no van a causar errores o incompatibilidades con otros sistemas o aplicaciones.

El uso de copias de seguridad actualizadas también se ha desvelado clave para hacer frente a este y cualquier otro ataque de ransomware, ahorrando así mucho tiempo a la hora de restaurar aquellos equipos que se hayan visto afectados.

También se ha de revisar que se cuenta con la última versión de las soluciones de seguridad implementadas tanto en estaciones de trabajo como en servidores y en la defensa perimetral, y que están debidamente configuradas, puesto que es muy probable que no solo se pueda detectar el malware si no que también se bloquee el exploit gracias a módulos específicos que analicen el tráfico de red para prevenir esta y otras vulnerabilidades.

¿Cómo ocultan los piratas informáticos sus direcciones IP?

Cuando nos conectamos a Internet, aunque no lo sepamos, dejamos constancia de una gran cantidad de datos que fácilmente pueden ser asociados a nuestra identidad. Algunos de estos datos son, entre otros, las huellas digitales, la dirección MAC de nuestra tarjeta de red y, sobre todo, la IP de nuestro ordenador. Como todo lo relacionado con el hacking está mal visto, incluso aunque sea con fines éticos, los hackers, igual que los piratas informáticos deben proteger su identidad ocultando esta información al conectarse a Internet, sobre todo, la dirección IP.

La **dirección IP** es la que identifica directamente nuestro ordenador en la red. A grandes rasgos, cuando enviamos un paquete de red a un servidor remoto, dentro de este se encuentra nuestra IP para que este servidor sepa dónde enviar la información de vuelta. Las compañías telefónicas suelen guardar un registro con todas las IPs que se asocian a cada usuario para que, en caso de denuncias o problemas, se pueda identificar al responsable.

A la hora de ocultar una dirección IP existen varias formas de hacerlo. A continuación, vamos a ver las 3 más utilizadas.

Conectarnos a Internet a través de Proxy

La forma más sencilla de conectarnos a Internet de forma anónima y privada ocultando nuestra IP es a través de un **Proxy.** De esta manera, establecemos una conexión directa con un servidor remoto y enviamos todo el tráfico a este, siendo el otro en responsable de reenviar el tráfico de red hasta su destino.

Algunos proxies conocidos son:

- BuyProxies
- HideMyAss
- MyPrivateProxies
- YourPrivateProxy
- EZProxies
- Anonymous-Proxies
- LimeProxies
- SSLPrivateProxy
- NewIPNow
- ProxyNVPN
- SquidProxies

Los Proxy, por lo general, aunque ocultan la dirección de red del usuario que se conecta a él, no es lo más seguro, por lo que no es recomendable más allá de simplemente ocultar nuestro país de origen para poder acceder, por ejemplo, a contenidos bloqueados regionalmente.Si queremos un anonimato superior debemos optar, por ejemplo, por un VPN.

Conectarnos a través de una VPN

Una conexión VPN es, a grandes rasgos, similar a la de un Proxy, con la diferencia de que **el tráfico entre nosotros y el servidor VPN se cifra**, evitando dejar el más mínimo rastro de él por la red. Existen muchos servidores VPN diferentes, y cada uno se avala por unas leyes, por lo que, si de verdad queremos ocultar nuestra identidad, debemos leer detenidamente los términos del servicio que utilizamos.

Reenviar nuestro tráfico a través de la red Tor

Por último, la medida más recomendable y utilizada cuando hablamos de hacking es la red **Tor.** Esta red cifra todo el tráfico en nuestro ordenador, oculta nuestra IP real y reenvía todo el tráfico a través de esta red distribuida de nodos. Todo el tráfico viaja cifrado hasta el nodo de salida y, además, debido al gran número de saltos que se realizan entre nodos, es muy complicada de rastrear.La red Tor es gratuita para todos los usuarios y podemos acceder a ella muy fácilmente utilizando simplemente Tor Browser. Además, con unas pequeñas configuraciones podemos hacer que absolutamente todo el tráfico de nuestro ordenador viaje cifrado a través de esta red.