WANNACRY: ATAQUE MUNDIAL Y CONSIDERACIONES SOBRE CIBERSEGURIDAD

Sergio Anduin Tovar Balderas
Raúl Abraham González Ponce
Demian García

wannacry

numero-29

El viernes 12 de mayo de 2017 se detectó un secuestro de equipos a escala mundial debido a una explotación de la vulnerabilidad de SMB (MS17-101) en las diferentes versiones de la familia de sistemas operativos Microsoft Windows. Este protocolo es utilizado para realizar tareas cotidianas, como compartir impresoras y archivos en entornos de trabajo y también en redes caseras. La amenaza que explotó esta vulnerabilidad fue un *ransomware*, es decir, un código malicioso que cifra la información del usuario y exige un rescate para restaurar los archivos, identificado en el medio como WannaCry.

El *malware* se propagó en muy poco tiempo a través del mundo. A primeras horas del viernes 12 diversas compañías en España reportaban computadoras secuestradas, entre ellas la compañía de telecomunicaciones Telefónica (Palazuelos, 2017a). Al mismo tiempo, en el Reino Unido se emitió un aviso a los usuarios del Sistema Nacional de Salud para anunciar que 40 hospitales habían sido afectados, por lo que en algunos de ellos se abstuvieron de prestar servicios de emergencia e incluso tuvieron que regresar al papel, lo cual causó demoras en la asistencia médica (Woollaston, 2017).

El mismo viernes el Centro Criptológico Nacional de España lanzó un informe en el que identificaba la especial criticidad de la campaña de ransomware (CCN-CERT, 2017). El malware incorpora características de un gusano y se propaga a través de la red explotando la vulnerabilidad en SMB (MS17-010) gracias al uso de los *exploits* EtneralBlue y DoublePulsar, dadas a conocer por el grupo ShadowBrokers (Paganini, 2017).

Esta vulnerabilidad era de conocimiento de Microsoft, por lo que en marzo de 2017 puso a disposición de los usuarios las actualizaciones de seguridad que solucionaban la vulnerabilidad en SMBv1 en el

boletín de seguridad MS17-010 (Microsoft, 2017b; Pagnotta, 2017). Sin embargo, la cantidad de dispositivos infectados en el mundo llegó a aproximadamente 300,000 en más de 179 países en tan solo 4 días (Palazuelos, 2017b), lo cual reveló la gran cantidad de dispositivos que usaban una versión de Windows sin las actualizaciones de seguridad más recientes. Más adelante se descubrió que al menos dos tercios de los dispositivos infectados en el ataque de ransomware usaban Windows 7, que no contaba con los parches de seguridad necesarios (Auchard, 2017). El mismo día del ataque, Microsoft tomó una decisión poco común y ofreció actualizaciones de seguridad gratuitas para las versiones anteriores a Windows 10 que presentaban un grado crítico de amenaza (Microsoft, 2017).

¿CÓMO FUNCIONA?

El funcionamiento general del ransomware WannaCry (también conocido como WannaCrypt, WCry, WanaCrypt0r, WCrypt o WCRY) es el siguiente:

1. WannaCry realiza una conexión a hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com. Si la conexión es exitosa hará que el malware se cierre (interruptor de apagado/kill switch).
2. Se ejecuta como servicio:
    1. Copia y mueve archivos del sistema.
    2. Tiene la capacidad de escanear el puerto 445 sobre TCP que ocupa el protocolo SMB en redes internas y en Internet con equipos e intenta propagarse vía SMB utilizando los exploits (EternalBlue/DoublePulsar).
3. Extrae un archivo zip que contiene la configuración de Tor que utiliza el malware para consultar los nodos Tor (.onion) que se utilizaran para la comunicación y cargar las carteras Bitcoin que son utilizadas para el pago del rescate.
4. Prepara los archivos, llaves públicas y privadas que utilizará para cifrar los archivos del equipo víctima.
5. Cifra los archivos y pide rescate en la criptomoneda Bitcoin.
6. Configura la persistencia.

Cabe mencionar que surgieron variantes de WannaCry que:

- No tenían kill switch
- Realizaban conexiones a dominios diferentes
- Consultaban nuevos nodos Tor (C2)

El ransomware cifra la información del usuario, principalmente documentos de audio, video, certificados, hojas de cálculo, imágenes, entre otros que se muestran a continuación.

.doc, .docx, .docb, .docm, .dot, .dotm, .dotx, .xls, .xlsx, .xlsm, .xlsb, .xlw, .xlt, .xlm, .xlc, .xltx, .xltm, .ppt,

.pptx, .pptm, .pot, .pps, .ppsm, .ppsx, .ppam, .potx, .potm, .pst, .ost, .msg, .eml, .edb, .vsd, .vsdx, .txt, .csv, .rtf, .123, .wks, .wk1, .pdf, .dwg, .onetoc2, .snt, .hwp, .602, .sxi, .sti, .sldx, .sldm, .sldm, .vdi, .vmdk, .vmx, .gpg, .aes, .ARC, .PAQ, .bz2, .tbk, .bak, .tar, .tgz, .gz, .7z, .rar, .zip, .backup, .iso, .vcd, .jpeg, .jpg, .bmp, .png, .gif, .raw, .cgm, .tif, .tiff, .nef, .psd, .ai, .svg, .djvu, .m4u, .m3u, .mid, .wma, .flv, .3g2, .mkv, .3gp, .mp4, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf, .wav, .mp3, .sh, .class, .jar, .java, .rb, .asp, .php, .jsp, .brd, .sch, .dch, .dip, .pl, .vb, .vbs, .ps1, .bat, .cmd, .js, .asm, .h, .pas, .cpp, .c, .cs, .suo, .sln, .ldf, .mdf, .ibd, .myi, .myd, .frm, .odb, .dbf, .db, .mdb, .accdb, .sql, .sqlitedb, .sqlite3, .asc, .lay6, .lay, .mml, .sxm, .otg, .odg, .uop, .std, .sxd, .otp, .odp, .wb2, .slk, .dif, .stc, .sxc, .ots, .ods, .3dm, .max, .3ds, .uot, .stw, .sxw, .ott, .odt, .pem, .p12, .csr, .crt, .key, .pfx, .de

KILLSWITCH

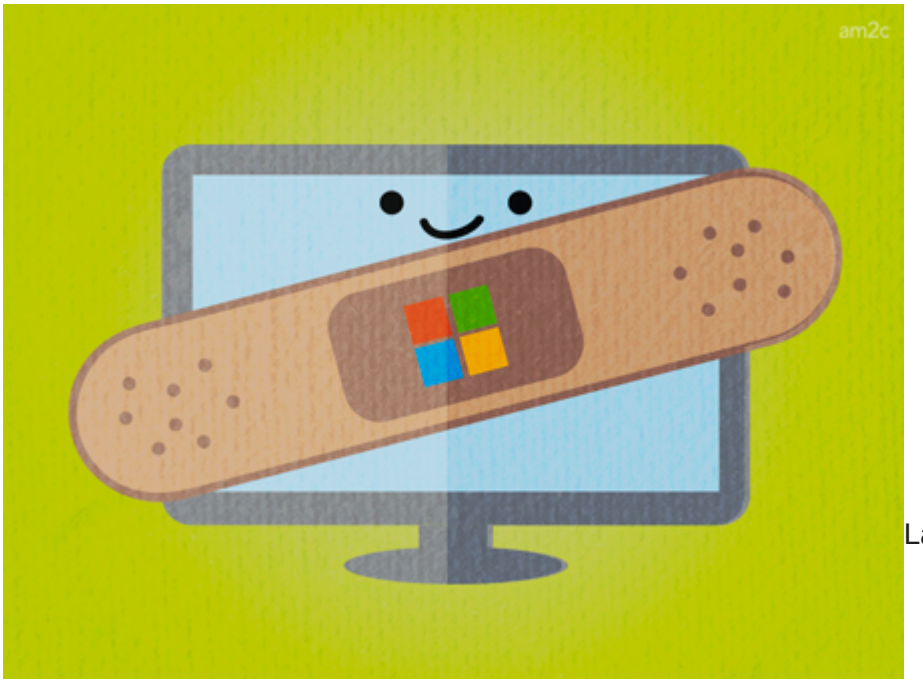
El sábado 13 de mayo un investigador de 22 años notó que las muestras del malware enviaban peticiones a un dominio. “Vi que no estaba registrado y pensé ‘quizá debería tenerlo’”, escribió Marcus Hutchins, cuyo nombre en Twitter es MalwareTech, así que compró el dominio por cerca de 10 dólares para analizar más tarde la relación entre el código malicioso y el DNS que había adquirido (Hutchins, 2017).

Marcus Hutchins explica que al principio creyó que al registrar el dominio había activado el ransomware, lo cual significaba que había cifrado la información de todo mundo. Sin embargo, el investigador de Proofpoint, Darien Huss, descubrió que en realidad al registrar el dominio la propagación de WannaCry se había frenado.

Durante el análisis de malware se identificó que se realizaba una consulta al dominio antes mencionado, y si no se obtenía respuesta, el ransomware continuaba buscando equipos vulnerables en la red para propagar la infección. Una vez registrado el dominio, los investigadores se dieron cuenta de que la muestra dejaba de propagarse por medio de la red. Esto significaba que la respuesta del dominio funcionaba como un interruptor de apagado o *killswitch*.

El sábado 13 de mayo algunos creyeron que el código malicioso se había detenido, pero aún se tenían sospechas de que el malware atacara de nuevo en otras versiones (Iglesias, 2017). El domingo se detectaron nuevas versiones de WannaCry que no necesitaban comunicarse con el dominio que hacía las funciones de killswitch, pero que seguían explotando la misma vulnerabilidad.

PARCHES DE SEGURIDAD PARA TODOS



La explotación de la vulnerabilidad de SMBv1 fue posible gracias a EternalBlue, que se hizo público a mediados de 2016. Esta vulnerabilidad fue parchada por Microsoft en el mes de marzo, para Windows 10. Sin embargo, los parches de seguridad no estaban disponibles para todas las plataformas Windows que están en soporte personalizado, incluidos Windows Xp, Windows 8 y Windows Server 2003.

Pero ante la propagación masiva, la compañía tomó un paso muy inusual al proporcionar la actualización de seguridad a todos sus sistemas operativos. Para los que utilizan Windows Defender se lanzó una actualización que detecta esta amenaza como “Win32/WannaCrypt”. El 22 de mayo liberaron una actualización de la Herramienta de eliminación de software malintencionado de Microsoft (MSRT) para detectar y eliminar el malware WannaCrypt (Warren, 2017; Microsoft, 2017a). Al mismo tiempo, las compañías de ciberseguridad actualizaron sus sistemas para detectar y mitigar esta amenaza.

EL CRIMEN NO PAGA

Los pagos realizados a los responsables de WannaCry, hasta el día 30 de mayo de 2017 rondaban los 110 mil dólares, de acuerdo con el rastreo de las transacciones realizadas a los tres monederos para recibir bitcoins identificados en el análisis del código malicioso. De acuerdo a las transacciones registradas en Blockchain se pagó por 336 rescates de información.

El balance final de este ataque indica que resultó poco redituable para los perpetradores, aunque bastante efectivo en su propagación, tomando en cuenta que más de 200,000 equipos en el mundo fueron infectados.

MEDIDAS PREVENTIVAS CONTRA WANNACRY Y OTRAS AMENAZAS CIBERNÉTICAS

A pesar de que esta amenaza fue contenida, es necesario mantener la guardia alta para no ser afectado por otros tipos de ransomware. Las recomendaciones básicas para estar preparado son:

1. Hacer respaldos de la información periódicamente.
2. Mantener actualizado el sistema operativo e instalar los parches de seguridad.
3. No abrir correos electrónicos de remitentes desconocidos ni abrir los archivos adjuntos.
4. No abrir enlaces de dudosa procedencia a menos de estar seguro de la confiabilidad de quien lo publica.
5. Mantener actualizado nuestro sistema *anti-malware*.

Si eres víctima del ransomware, la primera recomendación es no pagar el rescate ya que no hay garantía de obtener la información secuestrada. Al tener respaldos organizados y seguros podrás formatear la computadora para reinstalar los programas y recuperar tu información.

Puedes ver a continuación el video de como el ransomware WannaCry se apodera de un sistema Windows.

REFERENCIAS

- Auchard, E. (2017, 23 de mayo). Security experts find clues to ransomware worm's lingering risks. Reuters. Recuperado el 24 de mayo de 2017 de http://www.reuters.com/article/us-cyber-attack-failures-idUSKCN18E2SG?feedType=RSS&feedName=technologyNews&ct=t()
- CCN-CERT. (2017, 12 de mayo). Identificado ataque de ransomware que afecta a sistemas Windows. CCN-CERT. Recuperado el 24 de mayo de 2017 de https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html
- Cisco. (2017, 18 de mayo). Player 3 Has Entered the Game: Say Hello to 'WannaCry'. Recuperado el 18 de mayo de 2017 de http://blog.talosintelligence.com/2017/05/wannacry.html
- Endgame. (2017). WCry/WanaCry Ransomware Technical Analysis. Recuperado el 18 de mayo de 2017 de https://www.endgame.com/blog/technical-blog/wcrywanacry-ransomware-technical-analysis
- Hutchins, M. (2017, 13 de mayo). How to Accidentally Stop a Global Cyber Attack. MalwareTech. Recuperado el 25 de mayo de 2017 de https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html

- Iglesias, A. (2017). WannaCry: se confirma la existencia de 2 variantes del ransomware, que ya está remitiendo. TICbeat. Recuperado el 25 de mayo de 2017 de http://www.ticbeat.com/seguridad/wannacry-se-confirma-la-existencia-de-2-variantes-del-ransomware-que-ya-esta-remitiendo/
- Microsoft. (2017a, 12 de mayo). Customer Guidance for WannaCrypt attacks. Recuperado el 18 de mayo de 2017 de https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
- Microsoft. (2017b, 14 de marzo). Microsoft Security Bulletin MS17-010 – Critical. Microsoft TechNet. Recuperado el 25 de mayo de 2017 de https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
- Paganini, P. (2017, 22 de abril). Hackers compromised thousands of Windows boxes using leaked NSA hack tools DOUBLEPULSAR and ETERNALBLUE. Security Affairs. Recuperado el 24 de mayo de 2017 de http://securityaffairs.co/wordpress/58217/hacking/doublepulsar-nsa-massive-attacks.html
- Pagnotta, S. (2017). WannaCryptor lo hizo: llegó el día en que todos hablaron de seguridad. We Live Security – ESET. Recuperado el 24 de mayo de 2017 de https://www.welivesecurity.com/la-es/2017/05/15/wannacryptor-todos-hablaron-de-seguridad/
- Palazuelos, F. (2017a, 13 de mayo). La solución al ciberataque que no fue atendida. El país. Recuperado el 24 de mayo de 2017 de http://tecnologia.elpais.com/tecnologia/2017/05/13/actualidad/1494661227_809039.html
- Palazuelos, F. (2017b, 15 de mayo). China descubre una nueva mutación del virus responsable del ciberataque mundial. El país. Recuperado el 24 de mayo de 2017 de http://tecnologia.elpais.com/tecnologia/2017/05/15/actualidad/1494835268_125044.html
- Warren, T. (2017). Microsoft issues ‘highly unusual’ Windows XP patch to prevent massive ransomware attack. The Verge. Recuperado el 26 de mayo de 2017 de https://www.theverge.com/2017/5/13/15635006/microsoft-windows-xp-security-patch-wannacry-ransomware-attack
- Woollaston, V. (2017, 15 de mayo). The NHS trusts and hospitals affected by the Wannacry cyberattack. Wired. Recuperado el 24 de mayo de 2017 de http://www.wired.co.uk/article/nhs-trusts-affected-by-cyber-attack

SI QUIERES SABER MÁS, CONSULTA:

- El futuro no pertenece a los antivirus
- Navegando al día
- Tendencias de seguridad 2017. ¿Estás preparado?
