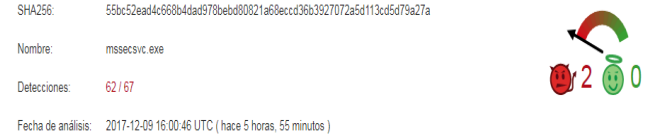
Variante WANNA CRYPT

El Comando Conjunto Cibernético informa que se ha detectado una campaña de ataques con una variante del Ransomware WannaCrypt, el cual trata de conectarse a diferentes IPs para descargar otra parte del virus en uno de sus clientes.


SHA256: 55bc52ead4c668b4dad978bebd80821a68eccd36b3927072a5d113cd5d79a27a

Nombre: mssecsvc.exe

Detecciones: 62 / 67

Fecha de análisis: 2017-12-09 16:00:46 UTC (hace 5 horas, 55 minutos)

mssecsvc.exe	190.198.189.235	Venezuela	microsoft-ds
mssecsvc.exe	59.91.136.208	India	microsoft-ds
mssecsvc.exe	59.90.50.177	India	microsoft-ds
mssecsvc.exe	120.163.95.157	Indonesia	microsoft-ds
mssecsvc.exe	68.186.219.117	EEUU	microsoft-ds
mssecsvc.exe	151.103.32.152	EEUU	microsoft-ds
mssecsvc.exe	173.98.213.207	EEUU	microsoft-ds
mssecsvc.exe	43.253.81.34	Japon	microsoft-ds
mssecsvc.exe	106.165.74.98	Japon	microsoft-ds
mssecsvc.exe	145.131.66.83	Países Bajos	microsoft-ds
mssecsvc.exe	134.176.156.46	Alemania	microsoft-ds
mssecsvc.exe	138.130.65.41	Australia	microsoft-ds
mssecsvc.exe	6.78.16.235	EEUU	microsoft-ds
mssecsvc.exe	190.6.36.39	Venezuela	microsoft-ds
mssecsvc.exe	130.167.239.29	EEUU	microsoft-ds
mssecsvc.exe	59.182.58.77	India	microsoft-ds
mssecsvc.exe	24.160.124.96	EEUU	microsoft-ds
mssecsvc.exe	130.0.193.118	Francia	microsoft-ds
mssecsvc.exe	22.200.185.47	EEUU	microsoft-ds
mssecsvc.exe	190.87.192.15	El Salvador	microsoft-ds

Es necesario trabajar en campañas para crear conciencia y alfabetizar cibernéticamente no sólo a los usuarios finales de los sistemas, para evitar ser víctimas de ataques como ransomware, sino también a los administradores y encargados de la seguridad para que mantengan una actitud diligente tendiente a prevenir incidentes informáticos mediante la actualización constante de sus sistemas operativos y herramientas de seguridad. De igual forma se requiere la creación y control de políticas de seguridad que puedan prevenir, detectar y contener cualquier tipo de amenaza cibernética que pongan en riesgo la integridad de los sistemas y de la información que en ellos se almacena y se procesa.

Identificación de archivo

MD5: e1872b7c2bd3cec6b2b4d963ea7b045c

SHA1: 0613b69a8e929dbdfd214459c36e3da59b7d5777

SHA256: 07feeb4eb206ece526a2c313a72abe47581a70176b409b05250fd7424d508505

IMPHASH: 9ecee117164e0b870a53dd187cdd7174

PEHASH: 3af6d1c60ca87a85045eec1e45e3fbb39348411b

RECOMENDACIONES

- Tenga una copia de respaldo de su información.
- ✓ Haga actualizaciones periódicas de su antivirus y del sistema operativo.
- ✓ Haga las actualizaciones de su sistema operativo. Para que estas sean efectivas su software debe ser legal. Consulte el catálogo de actualizaciones para Microsoft.
- ✓ Instalar el parche de emergencia KB4012598 para Windows y demás parches para solventar las vulnerabilidades aprovechadas por este ramsonware, dependiendo de la arquitectura y sistema operativo (MS017-010).
- ✓ Para las entidades o empresas que tengan equipos con sus sistemas operativos sin actualizar, lo mejor es desconectarlos de internet.
- ✓ Evite abrir correos electrónicos con archivos adjuntos sospechosos que aparentemente alerten sobre cobros jurídicos, demandas o similares.
- ✓ Si recibe un mensaje de alguna entidad bancaria o ente gubernamental, verifique que el dominio o link de la página web que se encuentre en el mensaje realmente sea el que represente oficialmente a la entidad o persona que se referencie.
- ✓ Nunca comparta información personal ni financiera solicitada a través de correos electrónicos, llamadas telefónicas, mensajes de texto o redes sociales.
- ✓ No abra mensajes ni archivos adjuntos de remitentes desconocidos.
- ✓ Tenga cuidado con los sitios web que visite, desconfíe de los dominios que no conozca.
- ✓ No descargue software de sitios no confiables.
- ✓ No descargue contenido multimedia por redes de intercambio.
- ✓ Evite conectar dispositivos extraíbles que no sean confiables.

Fuentes:

https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4488-informe-del-ransomware-de-la-familia-wannacry-que-incluye-medidas-para-su-deteccion-y-desinfeccion.html

https://otx.alienvault.com/indicator/file/55bc52ead4c668b4dad978bebd80821a68eccd36b3927072a5d113cd5d79a27a

https://www.virustotal.com/es/file/55bc52ead4c668b4dad978bebd80821a68eccd36b3927072a5d113cd5d79a27a/analysis/

Cualquier duda o inquietud comunicarse con el Comando Conjunto Cibernético-CCOC al teléfono 3150111 EXT 3087 o al correo ccoc@ccoc.mil.co