POLICÍA NACIONAL

UNIDAD DE DELITOS ESPECIALIZADOS Y VIOLENTOS UDEV/GRUPO DELITOS INFORMÁTICOS

UNIDAD DE PARTICIPACIÓN CIUDADANA POLICÍA NACIONAL JEREZ

VIRUS ENCRIPTADOR DE ARCHIVOS EMOTET PARA PEDIR RESCATE

La Policía Nacional informa de las características básicas y posibles medidas preventivas contra la proliferación en las últimas fechas de virus informáticos tipo troyano Emotet en la zona sur de españa incluído Jerez y su área de influencia.

Estos programas son diseñados específicamente para infectar sistemas de empresas e instituciones, encriptar con códigos muy complejos los archivos y sistemas operativos con la intención de chantajear a los afectados para pedirles un "rescate" a cambio de la clave de desencriptación.

Pagar nunca es la solución ya que se promueve el delito y además los delincuentes seguirán extorsionando a las empresas y particulares que cedan en un primer momento.

Como en la gran mayoría de otro tipo de malware de estas características el medio de infección es mediante correos electrónicos (e-mail) que los delincuentes lanzan de forma masiva.

Por esta razón una de las protecciones esenciales es que los empleados y operarios NO ABRAN NUNCA CORREOS DE DIRECCIONES DESCONOCIDAS Y MUCHO MENOS EJECUTEN ARCHIVOS ADJUNTOS O CLIQUEN EN "LINKS" INSERTADOS EN EL CUERPO DEL TEXTO DEL MAIL.

En este último caso la protección es mas difícil ya que el propio virus entra en los archivos de contacto de mail de la cuenta infectada y se reenvía a todos los contactos, suplantando su identidad "e-mail", dentro del correo viene un archivo de texto WORD ejecutable, sin embargo esta archivo de texto no contiene en sí el virus sino que lleva insertado un MACRO, que es una conexión que abre una conexión ON LINE que va descargando el troyano en segundo plano.

Normalmente el programa WORD de todo usuario te avisa si un texto, al abrirlo (ejecutarlo), lleva adjunto un MACRO de este tipo, pero la gran mayoría de los usuarios no le dan importancia y, cuando sale la pestaña de aviso, se clica siempre un "si", en este caso es un craso error.

De todas formas los modos de los delincuentes con sus mails son siempre cambiantes, hay casos incluso (no este) que el virus adjunto se puede descargar por el simple hecho de abrir un correo, sin ni siquiera ejecutar un archivo adjunto.

POR LO TANTO AHORA NO SOLO ES IMPORTANTE NO ABRIR ARCHIVOS ADJUNTOS A MAILS SINO TAN SIQUIERA ABRIR LOS PROPIOS MAILS DESDE LA BANDEJA DE ENTRADA, ANTE LA MÍNIMA SOSPECHA ENVIARLO DIRECTAMENTE A LA PAPELERA DE RECICLAJE Y VACIAR ESTA.

Otro consejo esencial para poder restaurar el sistema en caso de infección ES TENER UNA COPIA DE SEGURIDAD OFF LINE RAZONABLEMENTE ACTUALIZADA tanto del sistema como, y más importante, de todo los archivos de los discos duros, para ello es necesario mentener esta copia en un equipo TOTALMENTE AISLADO DE LA RED, NO CONECTADO NI POR CABLE NI POR WIFI.

Para más información remitimos al informe difundido por los expertos del CNI a traves del Centro Criptológico Nacional CCN sobre esta amenaza concreta.

Prevención frente a la campaña de código dañino EMOTET

- El CCN-CERT publica un informe de amenazas en la parte pública del portal del CCN-CERT.
- El objetivo del informe IA-51/19 es divulgar las medidas necesarias para prevenir la campaña de acción por parte del código dañino EMOTET, la cual está afectando de forma significativa a los sistemas de la información.
- Entre los principales puntos que se incluyen se encuentra el vector de ataque, las consecuencias, los mecanismos de prevención aplicables a través de los documentos de seguridad CCN-STIC para el ENS en su categoría alta, dispersión y movimientos literales, así como otras medidas.

El CERT del Centro Criptológico Nacional (CCN-CERT) ha publicado un nuevo Informe de Amenazas en la parte pública de su portal. El documento IA-51/19 tiene como principal misión la prevención de la campaña de código dañino EMOTET con medidas técnicas de las guías CCN-STIC de ENS nivel ALTO.

El punto de entrada o infección del código malicioso EMOTET se produce mediante la ejecución de código embebido desde un documento ofimático a través de aplicaciones tales como MS Word. Algunas de las consecuencias, una vez que la acción maliciosa se ha producido, son el proceso de secuestro del sistema mediante el cifrado del contenido, el robo y exfiltración de contenido sensible o

formar parte de una red de tipo “botnet”.

Como prevención, el CCN-CERT recomienda que se tomen en consideración todas aquellas medidas que, siendo de aplicación en los sistemas de la información, quedan recogidas en las guías técnicas de seguridad CCN-STIC que mejoran la seguridad y podrían prevenir su actuación. Específicamente, las medidas de seguridad a tener en cuenta están recogidas en las guías CCN-STIC-599A18 y CCN-STIC-585.

Adicionalmente, no deben desdeñarse otras potenciales medidas que ofrecerían la protección adecuada, como:

- Aplicar mecanismos integrales de protección Endpoint con análisis y protección frente a comportamientos dañinos que ofrezcan una medida preventiva adicional a la detección basada en firmas.
- Aplicar mecanismos de protección en el perímetro, con prevención frente a conexiones internas a sitios de contenido malicioso o de mando y control.

CCN (08/10/2019)

Adjuntamos enlaces de los informes del CNI:

https://www.ccn.cni.es/index.php/es/actualidad-ccn/481-prevencion-frente-a-la-campana-de-codigo-danino-emotet

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4119-ccn-cert-ia-51-19-prevencion-de-la-campana-de-codigo-danino-emotet-con-medidas-tecnicas-de-las-guias-ccn-stic-de-ens-nivel-alto-1/file.html

Ante cualquier duda, sospecha o incidencia, contactar con la Unidad de Participación en el teléfono 956326986, en la centralita de Comisaría 956326965 o al 091 ante cualquier incidente de caracter urgente.