CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

QUÉ ES EMOTET Y CÓMO PROTEGERSE

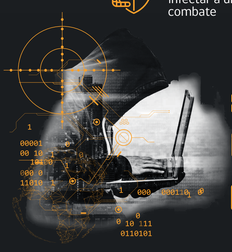
EMOTET ES UNO DE LOS MALWARE MÁS PELIGROSOS DEL MUNDO.

Ha evolucionado de ser un troyano bancario que interceptaba los datos de acceso de los clientes a servir como puerta trasera para todo tipo de delitos.

ESTE MALWARE SE DISEMINA PRINCIPALMENTE A TRAVÉS DE SPAM MALICIOSO COMO:

- Campañas de spam consistentes en emails con archivos adjuntos infectados, a través de documentos PDF, Word o Excel, o un link para descargar.
- Estos correos simulan contener información importante, como facturas o avisos de despacho.
- Al abrir el archivo, el malware se ejecuta automáticamente en el equipo.

Sus características son similares a un gusano, lo que le permite propagarse con rapidez para infectar a una red, por lo que no es sencillo su combate



ENTRE SUS PRINCIPALES OBJETIVOS ESTÁN:

- Extender su presencia en la mayor cantidad de dispositivos como le sea posible
- Distribuir correos electrónicos maliciosos para infectar a otras organizaciones
- Descargar y ejecutar una carga útil de malware en los dispositivos infectados

EMOTET PUEDE DESARROLLAR LAS SIGUIENTES FUNCIONALIDADES:

1. Robo de dinero desde cuentas bancarias
2. Propagarse a través de una red de recursos compartidos
3. Enviar campañas de phishing desde hosts infectados
4. Robar el historial de navegación y contraseñas del navegador
5. Robar credenciales de navegador web y clientes de correos utilizando software legítimos
6. Descargar y ejecutar otras familias de malware, generalmente troyanos bancarios

¿POR QUÉ ES TAN PELIGROSO?

1. Su código cambia cada vez que es usado y se expande con facilidad
2. Detecta cuando los expertos tratan de analizarlo en ambientes controlados como sandbox
3. Es un malware de servicios, es de fácil adquisición en el mercado negro de internet
4. Modifica una parte de su código para no ser detectado por las protecciones de seguridad.

PRINCIPALES CONSECUENCIAS DE EMOTET:

1. Pérdida temporal o permanente de información confidencial
2. Interrupción de las operaciones regulares
3. Pérdidas financieras para restaurar sistemas y archivos
4. Daño potencial a la reputación de una organización.

CÓMO EVITAR LA INFECCIÓN CON EMOTET

- No descargar archivos de emails desconocidos o hacer clic en sus enlaces.
- Mantener equipos y programas actualizados con los más recientes parches de seguridad.
- Si administra un sitio web, revisar periódicamente los equipos, ya que podrían estar infectados con malware.
- Realizar campañas de concientización para identificar ataques de phishing.

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Teatinos 92 piso 6
Santiago, Chile
www.csirt.gob.cl

Síguenos en nuestras redes sociales
Infórmate sobre nuestras actividades y escríbenos directamente