MINISTERIO DE SALUD PÚBLICA
Dirección Nacional de Seguridad y Protección
Calle 23 No. 201 e/ N y M, Vedado. La Habana

La Habana 5 de febrero del 2020
¨Año 62 de la Revolución ¨

A: Directores de Unidades de Subordinación Nacional.

Directores Provinciales de Salud.

Rectores de Universidades de Ciencias Médicas.

Estimados compañeros.

Por este medio se le comunica Alerta de Seguridad, por nueva campaña de propagación del **troyano EMOTET**.

A partir de la segunda quincena del mes de enero de 2020, se observa un incremento en el territorio nacional, de la recepción de mensajes que intentar propagar el **troyano EMOTET.** Es des significar que periódicamente, y varias veces al año, estas campañas se vienen produciendo. Es necesario instruir a todos los usuarios sistemáticamente sobre este tipo de intentos de propagación del **troyano EMOTET.**

Esta Alerta sobre la nueva campaña de propagación del **troyano EMOTET**, **debe enviarse por quién corresponda, a las entidades que se le subordinan en todo el país.**

EMOTET es un troyano polimórfico (cambia automáticamente su código cada cierto tiempo o con acciones determinadas del dispositivo). Anteriormente este malware se consideraba del tipo bancario, hoy en día está integrado con varias funciones maliciosas debido a que consta de varios módulos que descarga de su servidor C&C (comando y control), a saber:

- Módulo de spam
- Módulo de robo de credenciales y contactos
- Módulo de gusano de red
- Módulo para visualizar las contraseñas del correo electrónico
- Módulo para visualizar las contraseñas del navegador web
- Módulo de conexión con la botnet

- Módulo de ataque de fuerza bruta por SMTP
- Módulo de obtención de información del sistema

Propagación.

La infección inicial se distribuye a través de spam de correo electrónico con la siguiente secuencia de eventos:

- Un correo electrónico no deseado con suplantación de identidad, cuyo origen es una cuenta de correo electrónico, conformada por un dominio conocido asociado a la cuenta del atacante. Ejemplo:

  osri.gob.cu kevin@swfs.co.za

- Un correo electrónico no deseado con suplantación de identidad, cuyo origen es una cuenta de correo electrónico, en ocasiones conocida, seguida de otra no conocida. Ejemplo:

  <xxx.xxx@dominio conocido xxx.xxx@dominio desconocido>

- Los correos electrónicos que llevan la carga útil, pueden contener la siguiente información:
  Desde: {dominio conocido asociado a cuenta del emisor con dominio desconocido; cuenta conocida asociada a cuenta del emisor con dominio desconocido} como señalamos anteriormente.

  Asuntos tales como, aunque pueden variar:

  Todos estarán en la reunión mañana.

  Protocolo de la reunión

  Documento #{número}

  Factura #{número}

  Orden #{número}

  Pago #{número}

  Factura de pago #{número}

Boleto #{número}

En su Documento #{número}

Su pedido #{número}

Tu boleto #{número}

Estimado cliente,

Para leer el documento por favor, abra el archivo adjunto y responder lo más pronto posible.

Saludos cordiales

TCR de asistencia al cliente

- Este correo contiene un documento adjunto en Microsoft Word o PDF. O un enlace en el texto del mismo.
- El documento contiene código VBA (Visual Basic para aplicaciones) que al ser ejecutado decodifica e inicia un script Powershell.
- El script Powershell luego intenta descargar y ejecutar Emotet desde múltiples fuentes de URL para obtener malware desde las páginas maliciosas.

Indicaciones

- Realice acciones de educación de usuarios empleando la presente **Alerta de Seguridad por nueva campaña de propagación del troyano EMOTET.**
- Ante la presencia de este tipo de correos, ***re enviarlos compactados y con la contraseña VIRUS, a la Empresa SEGURMATICA a la dirección de correos virus@segurmatica.cu, y notificar como está establecido a la dirección de Seguridad y Protección MINSAP.***
- Lo anterior se debe a que los sistemas de seguridad de SEGURMATICA eliminan el correo y no puede ser estudiado el programa maligno.
- Utilice un Sistema Operativo seguro. Si es posible, sustituya los sistemas Windows antiguos por las versiones más recientes.
- Considere una configuración más estricta de la pasarela de correo electrónico, para evitar la entrada de mensajes con estas características.
- Evite instalar programas no confiables o inseguros.

- Ejecute las actualizaciones del Sistema de forma segura.
- No abra ni ejecute archivos adjuntos por correo, chat, etc. procedentes de direcciones desconocidas o poco confiables.
- Nunca deshabilite las funciones de seguridad porque un correo electrónico o un documento lo dice
- Bloquear macros en documentos de Office.
- Ponga contraseñas seguras a su ordenador.
- Asegúrese de que los usuarios no tengan acceso de administrador predeterminado.
- No visite webs de hackeo, adultos, casinos online o de dudosa procedencia.
- Instalar un programa cortafuegos (Firewall).
- No permita utilizar su PC a otras personas.

Atentamente.