El presente documento es propiedad del **Centro Nacional de Ciberseguridad (CNCS),** y fue generado mediante el análisis de varias fuentes de terceras partes y una investigación del equipo CSIRT-RD.

ALERTA DE SEGURIDAD

- **TLP** Blanco
- **Tipo de incidente** Código Malicioso
- **Categoría** Malware
- **Nivel de peligrosidad** **ALTO**

DETALLES DE ALERTA

El Equipo Nacional de Respuesta a Incidentes CSIRT- RD ha detectado el resurgimiento del peligroso malware Emotet, el cual funciona mediante archivos adjuntos maliciosos enviados a través de correos electrónicos.

INDICADORES DE COMPROMISO (IoC)

Dominios

- hxxp[:]//www.avrworks.com/mail/0Z4GbaKuDTGprJ/
- hxxp[:]//www.babylinesl.com/catalog/iVsl6YvlylyX/
- hxxps[:]//physioacademy.co.uk/blog/Qs8QZTp0Z6nKf9YjVBMS
- hxxps[:]//unada.us/acme-challenge/3NXwcYNCa/
- hxxps[:]//automobile-facile.fr/wp-admin/QV/
- hxxps[:]//alebit.de/css/gqKtdKmTsC4iDh/
- hxxp://www[.]arkpp.com/ARIS-BSU/9K1/
- hxxps://217[.]182.143.248:8080/TQkFRAMZfUqzbpjaPxFXwUXmBYQnpWcWqlUXLozODmbzQJXwGQvLSBSBshHK
- hxxp[:]//www[.]arkpp.com/ARIS-BSU/9K1/

IP

93[.]184.220.29
178[.]79.208.1
104[.]208.16.90
61[.]61.127.68
217[.]182.143.248
185[.]4.135.27
192[.]99.251.50

Muestras de Mensajes:

RECOMENDACIONES

Es evidente que el uso del correo electrónico representa un vector de propagación importante para los ciberatacantes distribuir código malicioso, por consiguiente, se debe evitar abrir enlaces de procedencia dudosa o dar información comprometedora a través de estos medios. A continuación las siguientes recomendaciones a fines de minimizar incidentes de este tipo:

1. Realizar el análisis correspondiente para el bloqueo a los indicadores de compromiso indicados en este documento.
2. Recomendamos tener precaución al momento de acceder a enlaces o archivos adjuntos suministrados mediante medios de mensajería.
3. Mantener actualizadas las plataformas y sistemas de información, priorizando las actualizaciones para aplicaciones externas y servicios de acceso remoto.
4. Realizar campañas de concientización periódica a todos los usuarios de la institución.