INC-01123-T2W5

ALERTA DE SEGURIDAD

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 04 DE AGOSTO 2020

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

REPÚBLICA DIGITAL

REPÚBLICA DOMINICANA Con la gente y para la gente | MINISTERIO DE LA PRESIDENCIA

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

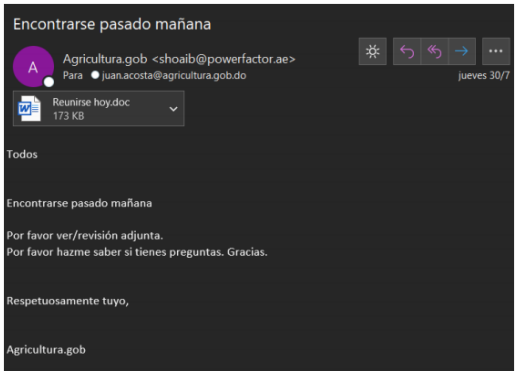
- **ID** INC-01123-T2W5
- **TLP** Blanco
- **Tipo de incidente** Ingeniería Social
- **Categoría** Robo de Información
- **Fecha de incidente** 31 de julio 2020
- **Fecha de reporte** 04 de agosto 2020
- **Nivel de peligrosidad** **Alto**

RESUMEN EJECUTIVO

Las organizaciones están expuestas a diferentes amenazas cibernéticas como consecuencia de la utilización de páginas web, aplicaciones móviles, correo electrónico, redes sociales, entre otras. La mayoría de estas amenazas están siendo diseñadas para el robo de información personal o corporativa con el objetivo de crear ataques cibernéticos. Dentro de los métodos comúnmente utilizados se encuentran el uso de correos electrónicos masivos con informaciones erróneas o con links para que el usuario realice acciones que tienen como principal objetivo capturar información o distribuir código malicioso en los equipos de los usuarios.

DETALLES DE LA ALERTA

A través de una notificación al correo de reportes de incidentes del Equipo Nacional de Respuestas a Incidentes Cibernéticos (CSIRT-RD), fue reportada una campaña de malware via correo electrónico con el asunto "**Encontrarse pasado mañana**" que contiene un archivo adjunto con el nombre **"Reunirse hoy[.]doc".**



Se ha analizado el archivo suministrado en un ambiente controlado y se observa que al ejecutarse se realizan procesos no autorizados por el usuario donde se ejecuta un programa malicioso conocido con el nombre **Emotet** que realiza algunas conexiones con IPs de diferentes países para intentar descargar y ejecutar archivos maliciosos.

INDICADORES DE COMPROMISO (IoC)

Remitente
shoaib@powerfactor[.]ae

Asunto
Encontrarse pasado mañana

Conexiones IP
67[.]20[.]112[[.]81
187[.]64[.]128[.]197
198[.]57[.]203[.]63
89[.]232[.]34[.]133

HASH
Archivo Principal: Reunirse hoy[.]doc
Sha256:
2855f5589490a4300a25a94c7b74abd2a9b72572
MD5: e4ea0954c68994b7e90f5f7b56a7b07f

Archivo Ejecutado: 90o38eznv72[.]exe
SHA256:
9c2e60be8b09806bf0f9079d5e3c167cf15e06aaf8
b7ebd9147da78412c90b63
MD5: 76ade0ffedeeb4fbbd581cc4b051890f

Peticiones HTTP:

- http://jambino[.]us/tv/DYsPb/
- http://187[.]64[.]128[.]197/ksao2mre0PnE4t5C3/UPg8CQv6/w1bdTJ80els6wDRpIiZ/4hADF8Q/
- http://187[.]64[.]128[.]197/iMEB1aE/BUWn6X/
- http://187[.]64[.]128[.]197/GJiF/tnFPZ19hwM/oUJLjb/A58wj6w/a5yZKtTHV/
- http://187[.]64[.]128[.]197/Vbk6aAWoXA94nTYA/9s3isFHejlZbpEX5/GzCl475rZ/ppQkEGw9QOBx9a/qBOyswrC/
- http://187[.]64[.]128[.]197/2GNaDTxG1t7u9KWhU/jMrpdW8VjLuAe0/nGglHMuHTLyJffxUqu/AoMC/
- http://187[.]64[.]128[.]197/ASkyNOqpW/RfWGQkF9C/
- http://198[.]57[.]203[.]63/9GW1/aHDk6kIOkcU6gk/Ew5k0FqK3rs3kO121as/mAyArLVGeHOKf/Bh9fL4BkdmklbghvM/
- http://187[.]64[.]128[.]197/BlV81TaPKRRR7bbu/7EKeRMGtx7JwEpH6G/3wjojCY/
- http://187[.]64[.]128[.]197/YB7gbKty8iz/V3bFCEt/uRTyaCuvc/7bNKgXXBkU2hM/ZNlm/19875p4Pl2RtX97Os52/
- http://187[.]64[.]128[.]197/gsH8T/hYoQV52aF8vUl0c/mAYad9Ul5d2viu/yQTBw/
- http://187[.]64[.]128[.]197/XQSLxnFnxPRYg99b/e7I4T4IMNri359ztYBT/IDYJP1ltPe2FAbk/

1. Realizar el análisis correspondiente para el bloqueo a los indicadores de compromiso expuestos, indicados en este documento.
2. Recomendamos tener precaución al momento de acceder a enlaces o adjuntos suministrados vía correo electrónico
3. Mantener actualizadas las plataformas y sistemas de información.
4. Realizar campañas de concientización periódica a todos los usuarios de la institución.