CNCS | CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

REPÚBLICA DIGITAL

ALERTA DE SEGURIDAD

INC-01049-K6R2

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

Fecha de publicación: 13 de marzo 2020

ALERTA DE SEGURIDAD

ID	INC-01049-K6R2
TLP	Blanco
Tipo de incidente	Malware
Categoría	Código Malicioso
Fecha de incidente	13 de febrero 2020
Fecha de reporte	13 de marzo 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 malware o programa de código malicioso que tienen como objetivo dañar los sistemas de información, causar un mal funcionamiento o robar datos, ejecutando acciones no deseadas ni detectadas por los usuarios en el sistema.

DETALLES DEL INCIDENTE

A través de una notificación al correo de reportes de incidentes del Equipo Nacional de Respuestas a Incidentes Cibernéticos (CSIRT-RD), se ha identificado una campaña de malware vía correo electrónico que contiene un archivo malicioso adjunto con el nombre **CoronaVirusSafetyMeasures_pdf(.)exe** que invita al usuario abrir el documento.

Se ha analizado el archivo en un ambiente controlado y se observa que al ejecutarse se realizan procesos no visibles por el usuario que descarga un programa malicioso para infectar el equipo.

INDICADORES DE COMPROMISO (IoC)

Asunto:

"the mask that can prevent coronavirus now"
"coronavirus is spreading prótocolo de atención en clínica alemana"
"comunicado coronavirus "
"Corona is Spinning Out of Control"
"All STAFF: CORONA VIRUS AWARENESS"
"Urgent: WHO Coronavirus Update"

Conexiones IP:

185[.]212[.]128[.]231
66[.]154[.]98[.]108

Soluciones de DNS

Share[.]dmca[.]gripe

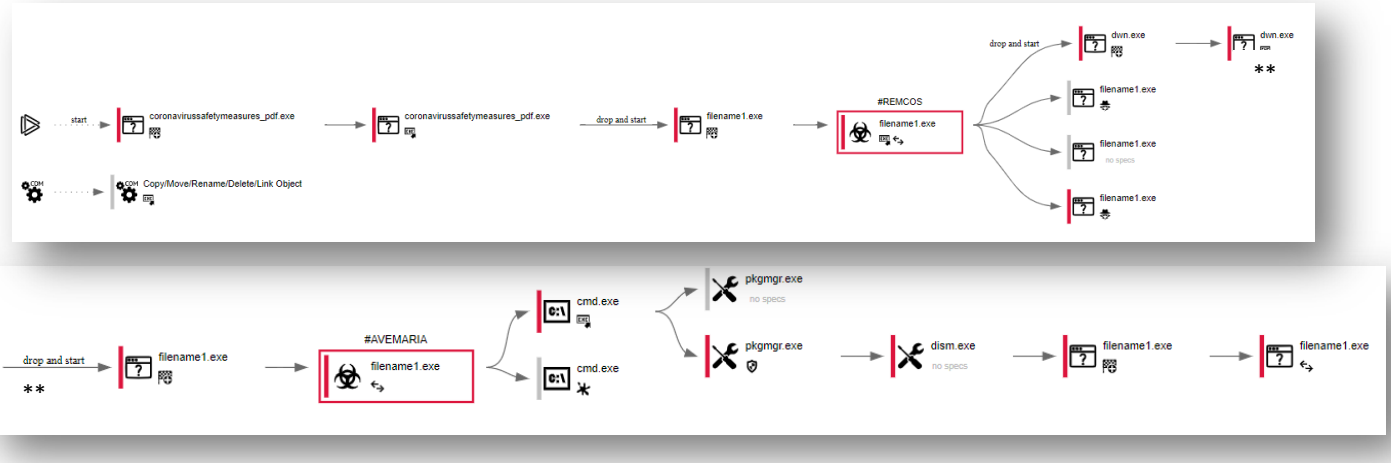
Hash

Archivo Principal:

"CoronaVirusSafetyMeasures_pdf"
SHA1 C87ED1AECB4936031222882B873AF31341B6DD69
MD5 A3042B64C0C3086B890CC3F6CFB334DD

Archivo secundario: "filename1.exe"

MD5: 61CE777555EE4D591FF151E0927AB8D4



Mitre ATT&CK, Técnicas de detección

Acceso Inicial	Ejecución	Persistencia	Escala de privilegios	Evasión de defensa	Acceso de credenciales	Descubrimiento	Movimiento Lateral	Colección
	Interface con la línea de comando	Claves de ejecución del registro / Carpeta de inicio		Instalar el certificado root	Credenciales en archivos	Registro de consulta		Colección de correos
	Ejecución de carga mediante API					Descubrir información del sistema		
	Ejecución de carga de módulos							

RECOMENDACIONES

1. Realizar el análisis correspondiente para el bloqueo a los indicadores de compromiso expuestos, indicados en este documento.
2. Mantener actualizadas las plataformas y sistemas de información.
3. Realizar campañas de concientización periódica a todos los usuarios de la institución.