

**sedian**

Seguridad Digital  
de Andalucía



Manual de usuario  
**Manual de compartición de indicadores de  
compromiso**

Tipo de documento: Manual de usuario

Autor del documento: AndalucíaCERT

Código del documento: CERT-MU-012-00

Edición: 0

Categoría: Uso interno por la Comunidad

Fecha de elaboración: 09/06/2020



## Hoja de control de ediciones

N.º. Edición	Fecha	Editor	Naturaleza de la edición
0	25/03/19	AASG	Edición inicial

### Detalles de los cambios de la última edición

### Lista de distribución

Nombre	Organización	Fecha
Organismos del Grupo Atendido	Organismos del Grupo Atendido	25/03/2019

Elaborado	Revisado	Revisado	Aprobado
AASG			MMJP
Responsable técnico AndalucíaCERT			Responsable Seguridad y Confianza Digital

# Tabla de contenidos

Tabla de contenidos.....	3
Compartición de indicadores de compromiso.....	4
Indicadores.....	4
Descarga de ficheros de listas negras.....	5
Descarga de ficheros de reglas SNORT.....	6
Muestra de acceso.....	7
Casos de uso.....	8
Normas de uso.....	8
Referencias.....	9

# Compartición de indicadores de compromiso

AndalucíaCERT presta a su comunidad un servicio de compartición de inteligencia de ciberamenazas mediante indicadores de compromiso (IOC - Indicator of Compromise) de fuentes internas y externas. Para simplificar y facilitar la usabilidad se pone a disposición de su Organismo una serie de listas negras de diversos tipos de indicadores con mala reputación y de reglas de detección de tráfico de red en formato SNORT. AndalucíaCERT actúa de intermediario de otros proveedores de fuentes de inteligencia, tanto públicos como privados.

La fuente privada utilizada es REYES. REYES (REpositorio común Y EStructurado de amenazas y código dañino) es una herramienta desarrollada por el CCN-CERT para agilizar la labor de análisis de ciberincidentes y compartir información de ciberamenazas. En un primer momento, REYES se basó en la tecnología MISP (Malware Information Sharing Platform), sin embargo, en su nueva versión ha pasado a ser un portal centralizado en el que se ha integrado un metabuscador, se ha implementado una API y se ha integrado con otras herramientas del CCN-CERT.

## Indicadores

Actualmente la información publicada se encuentra limitada a listas negras en formato texto y reglas SNORT.

# Descarga de ficheros de listas negras

Para descargar los ficheros de texto de las listas negras debe acceder al siguiente recurso:

<https://ioc.andcert.junta-andalucia.es/bl/<blacklist>>

Relación de ficheros de listas negras disponibles:

Fichero blacklist	Contenido
reyes-bl-botnet_ip.txt	Indicadores de direcciones IP relacionadas con botnets. Fuente: CCN-CERT REYES.
reyes-bl-botnet.txt	Indicadores de dominios relacionados con botnets. Fuente: CCN-CERT REYES.
reyes-bl-apt_ip.txt	Indicadores de direcciones IP relacionadas con amenazas avanzadas. Fuente: CCN-CERT REYES.
reyes-bl-apt.txt	Indicadores de dominios relacionados con amenazas avanzadas. Fuente: CCN-CERT REYES.
reyes-bl-malware_ip.txt	Indicadores de direcciones IP relacionadas con código malicioso. Fuente: CCN-CERT REYES.
reyes-bl-malware.txt	Indicadores de dominios relacionados con código malicioso. Fuente: CCN-

	CERT REYES.
reyes-bl-malware_url.txt	Indicadores de URL relacionados con código malicioso. Fuente: CCN-CERT REYES.
reyes-bl-spam.txt	Indicadores de direcciones IP relacionadas con SPAM. Fuente: CCN-CERT REYES.
public-blacklist_ip.txt	Indicadores de direcciones IP con mala reputación según diversos proveedores de seguridad reconocidos. Fuente: Abierta.
andaluciacert-brute-force_ip.txt	Indicadores de direcciones IP con comportamiento de ataque de credenciales por fuerza bruta contra servicios de Junta de Andalucía. Fuente: AndalucíaCERT.

Tabla 1. Listado de ficheros de listas negras.

## Descarga de ficheros de reglas SNORT

Para descargar los ficheros de reglas debe acceder al recurso:

<https://ioc.andcert.junta-andalucia.es/rule/<rules>>

Relación de ficheros de reglas disponibles:

Fichero rules	Contenido
reyes-ransomware.rules	Reglas de detección relacionadas con ransomware. Fuente: CCN-CERT REYES.
reyes-apt.rules	Reglas de detección relacionadas con amenazas avanzadas. Fuente: CCN-CERT REYES.

Tabla 2. Listado de ficheros de reglas snort.

## Muestra de acceso

Ejemplo de acceso a una lista negra a través de un navegador:



Imagen 1. Ejemplo de acceso a una lista negra.

Para un tratamiento automatizado se recomienda la descarga por línea de comando, mediante la utilidad wget o similar.

## Casos de uso

Estos indicadores se pueden utilizar para la contextualización o enriquecimiento de eventos de seguridad, así como en los sistemas de detección y prevención de amenazas, como pueden ser, por ejemplo: resolutores de DNS, pasarelas de navegación, cortafuegos, sensores de detección de intrusión de red o SIEM entre otros.

Antes de desplegar las listas en modo de prevención de amenazas, se recomienda encarecidamente evaluar previamente su compartimiento sin forzar el bloqueo.

## Normas de uso

A continuación se resumen las obligaciones de los suscriptores del servicio:

- Tratar los indicadores suministrados como información Confidencial - Difusión Restringida.
- Revisar los logs para detectar intentos de acceso a los indicadores suministrados.
- Gestionar los incidentes asociados y, si aplica, comunicarlos a AndalucíaCERT.

## Referencias

[1] Trabajadores del CCN-CERT. <<Guía de Seguridad (CCN-STIC-423). *Indicadores de Compromiso (IOC)*>>. Web oficial del CCN-CERT, octubre de 2015. Disponible en línea: <https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1090-ccn-stic-423-indicadores-de-compromiso/file.html>

[2] Trabajadores del CCN-CERT. <<Guía de Seguridad de las TIC (CCN-STIC-424). *Intercambio de Información de Ciberamenazas. STIX-TAXII. Empleo de REYES*>>. Web oficial del CCN-CERT, octubre de 2015. Disponible en línea: <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1105-424-intercambio-informacion-ciberamenazas-stix-taxii-oct15/file.html>

[3] Trabajadores del CCN-CERT. <<Guía de Seguridad (CCN-STIC-425). *Ciclo de Inteligencia y Análisis de Intrusiones*>>. Web oficial del CCN-CERT, octubre de 2015. Disponible en línea: <https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1093-ccn-stic-425-ciclo-de-inteligencia-y-analisis-de-intrusiones/file.html>

[4] Trabajadores del CCN-CERT. <<Guía de Seguridad de las TIC. CCN-STIC 426. *REYES. Manual de usuario*>>. Web oficial del CCN-CERT, noviembre de 2017. Disponible en línea: <https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1318-ccn-stic-426-reyes-manual-de-usuario-1/file.html>