TLP:GREEN

sedian

Seguridad Digital
de Andalucía

Presentación

Compartición de indicadores de compromisos

Tipo de documento: Presentación

Autor del documento: AndalucíaCERT

Código del documento: CERT-PS-012-00

Edición: 5

Categoría: Uso interno por la Comunidad

Fecha de elaboración: 09/06/2020

Junta de Andalucía

Compartición de indicadores de compromiso

AndaluciaCERT 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.

La información está disponible parar su descarga en un servidor web con control de acceso.

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