



Conferencia de InnoTec-Entelgy en BlackHat, referente mundial de Seguridad informática

Este año volvemos a estar de celebración.

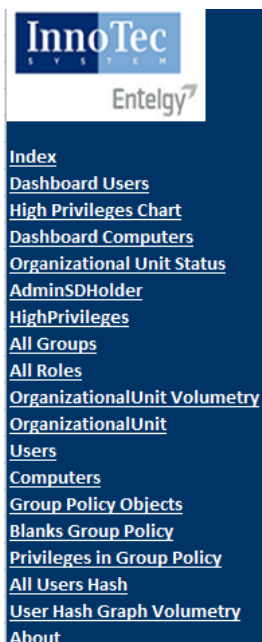
Entre las múltiples conferencias que nuestros compañeros de Innotec realizan a lo largo y ancho de este mundo, y por segundo año consecutivo, ha sido aceptada [una charla](#) en el prestigioso congreso de seguridad informática **BlackHat**, uno de los mayores y mejores eventos de todo el panorama mundial y en donde son pocos los españoles elegidos para

ofrecer una conferencia. Del 2 al 7 de agosto, en Las Vegas, se dan cita miles de expertos en seguridad de la información, en lo que representa un punto de reflexión para nuevos avances y tendencias, así como estudios, herramientas y metodologías.



En esta ocasión, el día 7, Juan Garrido, consultor especializado en análisis forense y test de intrusión, presentará una nueva herramienta **basada en metodología propia** de Innotec-Entelgy para auditorías de servicios basados en **Directorio Activo** (estructura jerárquica donde se establecen los recursos de la red, permisos, políticas...es decir, desde el directorio activo se controla toda la red de una organización). La herramienta, denominada **Voyeur**, será una inestimable ayuda a la hora de realizar con más rigor auditorías basadas en este tipo de servicios, considerados como infraestructuras críticas dentro de una empresa.

Según palabras de Juan, la herramienta nació a través de un caso de respuesta a incidentes. *“Hubo que mirar en una infraestructura replicada en múltiples países la creación de una serie de objetos, y el tiempo era crucial para dar respuesta a estas y otras preguntas que surgieron en aquel caso”*.



A día de hoy es una herramienta estable, estructurada y modular que permite, entre otras cosas, realizar peticiones a todo tipo de objetos en una infraestructura. La herramienta está íntegramente desarrollada en PowerShell y .NET, no requiriendo ningún tipo de dependencia para ser utilizada.

En cuanto a la parte de informes, la herramienta es capaz de poder pintar los datos extraídos de un servicio de Directorio Activo en una hoja de EXCEL, generando información de valor utilizando técnicas de data mining.

Ilustración 1. Algunos de los elementos extraídos por la herramienta



Históricamente, herramientas unitarias que extraen parte de esta información, sólo funcionan en servicios de un idioma predeterminado, como inglés o castellano (dos de los idiomas más instalados). Debido a esta problemática, nuestra herramienta funciona en servicios de Directorio Activo instalados en cualquier tipo de idioma.

High Privileges Accounts in Groups

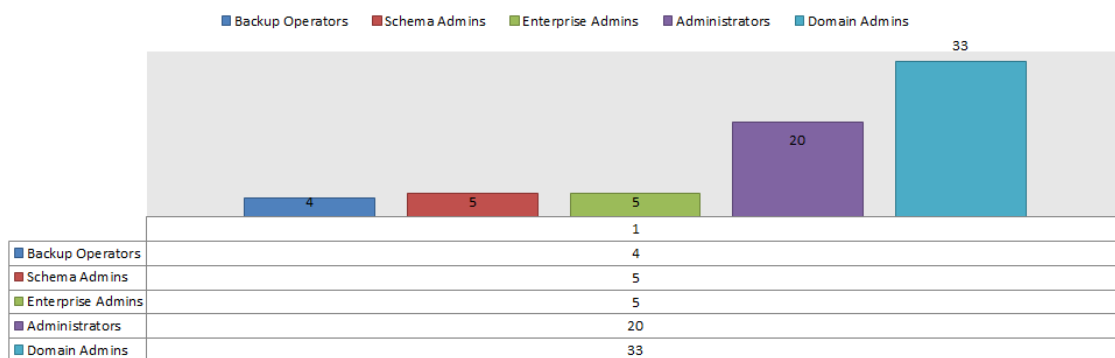


Ilustración 2. Una de las múltiples gráficas realizadas por la herramienta

Desde este post queremos dar las gracias a los chicos de Sistemas, Redes y Comunicaciones de Entelgy (¡gracias Jorge Talavera! 😊), que nos han ayudado a solucionar errores, así como a mejorar la misma.

Aunque el lema oficial de Las Vegas es “Lo que pasa en Las Vegas, se queda en Las Vegas”, desde Entelgy haremos caso omiso al mismo e iremos informando de las novedades que pudiesen ir surgiendo.

<https://www.blackhat.com/us-14/arsenal.html#Garrido>

<https://www.blackhat.com/us-14/arsenal/Juan-Garrido.html>