techWEEK.es

Impreso: martes, 02 de septiembre de 2014 - 10:40
URL: http://www.techweek.es/seguridad/noticias/1014320004801/innotec-entelgy-blackhat-herramienta-voyeur-auditorias-servicios.1.html

Innotec-Entelgy presenta en BlackHat la herramienta Voyeur para auditorías de servicios

02 Septiembre 2014

Por segundo año consecutivo, la filial de Entelgy especializada en ciberseguridad ha participado con una ponencia en BlackHat y aprovechó el congreso de seguridad para presentar Voyeur, una nueva herramienta para auditorías de servicios basados en Directorio Activo, estructura jerárquica donde se establecen los recursos de la red, permisos y políticas

“Participar, por segundo año consecutivo, en uno de los eventos de seguridad informática más importantes del mundo es una oportunidad única que permite conocer de primera mano las últimas tendencias, informes, herramientas y metodologías de vanguardia en el sector", asegura Juan Garrido, consultor especializado en análisis forense y test de intrusión de Innotec-Entelgy y encargado de representar a la compañía en el congreso.

Además, la firma de ciberseguridad aprovechó el marco de BlackHat para anunciar Voyeur, una nueva herramienta basada en metodología propia de la compañía para auditorías de servicios basados en Directorio Activo, estructura jerárquica donde se establecen los recursos de la red, permisos, políticas, etc: desde el directorio activo se controla toda la red de una organización.

Este sistema 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. El tiempo era crucial para dar respuesta a estas y otras preguntas que surgieron en aquel caso”, afirma Juan Garrido.

A día de hoy, Voyeur es una herramienta estable, estructurada y modular que permite, entre otras cosas, realizar peticiones a todo tipo de objetos en una infraestructura. Está íntegramente desarrollada en PowerShell y .NET, y no requiere ningún tipo de dependencia para su uso. En cuanto a la parte de informes, Voyeur es capaz de pintar los datos extraídos de un servicio de Directorio Activo en una hoja de Excel, generando información de valor utilizando técnicas de data mining.

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). Para resolver esta problemática, Voyeur funciona en servicios de Directorio Activo instalados en cualquier tipo de idioma.

Juan Garrido valora muy positivamente la puesta en escena de Voyeur: "La presentación en Black Hat de la herramienta tuvo una gran acogida entre los asistentes, muy preocupados por los posibles ataques al Directorio Activo, desde donde se puede controlar la red de cualquier organización. Gracias a esta herramienta se pueden realizar, con gran precisión, auditorías basadas en este tipo de servicios,

considerados críticos dentro de una empresa". Más información en www.blackhat.com/us-14/arsenal.html#Garrido