Xeración e distribución de malware

Descrición

Durante esta xornada mostraranse os mecanismos para xerar e distribuír malware empregados nas auditorías de hacking ético. Tamén se revisarán as últimas tácticas de análises de malware para ransomware, malware bancario e financeiro, botnets de IoT, análise de malware OT, malware de Android, etc.

Ademais, presentaranse os ataques fileless. Dado que o malware fileless é unha forma relativamente nova de ataque de malware, as organizacións teñen dificultades para detectalo con solucións de seguridade.

A xornada estará centrada na taxonomía das ameazas de malware, técnicas de ofuscación para evitar o antivirus, lanzar malware a través da inxección baseada en script e lanzar malware sen arquivos.

O relator da xornada será David Sierra Alegre, enxeñeiro de Telecomunicación e senior technical trainer en PUE. Certificado como formador de tecnoloxías EC-Council, conta con máis de 15 anos de experiencia como formador e consultor experto en redes, sistemas e ciberseguridade.

Como valor engadido, dende PUE, training partner oficial de EC-Council, xestionarase o acceso gratuíto a todos/as os/as asistentes á xornada a un practice test oficial de preparación da certificación Ethical Hacking Associate (EHA).

DURACIÓN 4 horas

METODOLOXÍA Virtual

BENEFICIOS

HORARIO O 01/06/2021 de 10:00 a 14:00 horas.

PROBA DE SELECCIÓN null

LUGAR DE DOCENCIA

Nº PRAZAS 500

Temario

- Últimas tácticas de análises de malware para ransomware
- Ataques fileless
- A taxonomía das ameazas de malware
- Técnicas de ofuscación para evitar o antivirus
- Lanzamento de malware a través da inxección baseada en script
- Lanzamento de malware sen arquivos