I SEMINARI DEL DII

CYBER master SECURITY

Attacchi avanzati basati su Powershell - Le nuove frontiere del malware

Giuseppe Mario Malandrone
Gavino Roberto Pinna
Alessandro Sanna
Numera Sistemi e Informatica S.P.A.

VENERDÌ 18 FEBBRAIO 2022
H 14:00

Abstract

Negli ultimi anni sono stati identificati numerosi attacchi informatici veicolati attraverso documenti Microsoft Office, che sfruttano le funzionalità di PowerShell e rappresentano una tipica applicazione della tecnica “living off the land”, in quanto uno strumento legittimo viene utilizzato per scopi malevoli. La diffusione di questo tipo di attacchi è legata essenzialmente alla possibilità offerta dalla shell di eseguire script in grado di caricare istruzioni in linguaggio macchina direttamente in memoria o capaci di stabilire una connessione verso un server remoto e dalla possibilità di applicare tecniche di offuscamento atte ad eludere le più comuni protezioni offerte dagli antivirus signature-based, cosa che rende i malware PowerShell un importante rischio per i sistemi Windows. Durante il seminario verranno analizzate le principali tecniche utilizzate in questa tipologia di attacchi e verrà fornita una panoramica sugli strumenti Oblivion e PowerDecode rispettivamente dedicati all'analisi dei documenti Microsoft Office e degli script Powershell.

Bio

Ing. Giuseppe Mario Malandrone - Security Specialist presso Numera Sistemi e Informatica S.p.A. - Laurea magistrale in Ingegneria Elettronica presso l'Università degli studi di Cagliari, autore del software "PowerDecode" per l'analisi dei malware Powershell; nel 2021 ha presentato il paper "PowerDecode a PowerShell Script Decoder Dedicated to Malware Analysis" all'evento nazionale ITASEC21 organizzato dal CINI. Classificato tra i primi partecipanti alla 16ma edizione del Premio Tesi «Innovare la sicurezza delle informazioni» organizzato dal CLUSIT.

Ing. Gavino Roberto Pinna - Security Specialist presso Numera Sistemi e Informatica S.p.A. - Laurea in Ingegneria Informatica presso l'Università degli studi di Pisa, autore, in collaborazione con il CISAM, del progetto per la reiezione dei falsi allarmi in un sistema di ricerca di materiale radioattivo su veicoli sospetti. Il sistema è stato testato all'interno del reattore nucleare di ricerca Galileo Galilei costituendo un'ampia rilevanza e affidabilità nel settore di sicurezza nazionale e militare. Finalista all'evento hackathon "Think Hack Restart" organizzato da INNOIS Srl e Open Campus con il progetto "Ambulatorio Virtuale" in collaborazione con il Dott. Ivan Raimondi.

Ing. Alessandro Sanna - Dottorando presso Numera Sistemi e Informatica S.p.A. - Tema dottorato: Evoluzioni, rilevamento e analisi dei malware powershell - Laurea magistrale in Ingegneria Informatica presso l'Università degli studi di Cagliari. Coautore del software "Oblivion" per l'analisi dei malware Powershell.

Per partecipare occorre registrarsi al link **https://forms.gle/r7c8CyWz24jt6FPp6**

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

In collaborazione con

ISTITUTO DI INFORMATICA E TELEMATICA

UNIVERSITÀ DI PISA