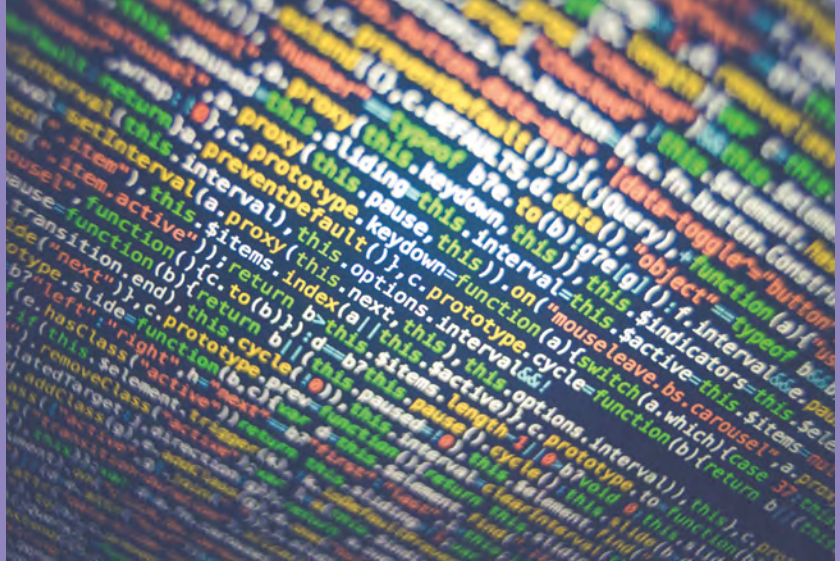
PRÄSENZ



MALWARE UNTERSUCHEN UND VERSTEHEN LERNEN

GRUNDLAGEN SCHADSOFTWARE-ANALYSE WINDOWS

Die Herausforderung: Erkennen der Schadsoftware und ihrer Funktionalität. Oft ist es nicht mehr ausreichend, nur festzustellen, ob sich ein Programm potenziell bösartig verhält oder nicht. Allein die exakte Bestimmung einer Malwarefamilie kann bereits eine Herausforderung sein, denn Malware liegt üblicherweise nur als fertig kompiliertes Programm im Maschinencode vor. Da nun also der Quellcode nicht verfügbar ist, sind schnell Spezialwissen wie auch Werkzeuge erforderlich, um Erkenntnisse über Fähigkeiten und Verhalten der Malware zu erarbeiten.

Inhalte des Seminars

Generelle Einführung zu Schadsoftware: Relevante Beispiele und die grundsätzliche Analysemethodik des Reverse Engineerings

Systemnahe Einführung zu Windows und der Umgang mit Virtualisierung als Schutzschicht

Oberflächliche Analysen durch Systembeobachtung

Überblick über die x86-/x64-Architektur und ein Schnellkurs zum Verständnis von Assemblern

Einführung in dynamische und statische Analysetechniken mit der Gelegenheit, diese im Rahmen von Botnet Takeovers in unserer Laborumgebung zu vertiefen

Ihr Nutzen

» Nach dem Seminar können Sie Angriffsvektoren von Schadsoftware besser einschätzen.
» Sie können Analysen durchführen, um einen grundsätzlichen Eindruck von Schadsoftware zu erhalten.
» Sie kennen typische Analysetools wie Debugger und IDA Pro und können diese anwenden.

INFORMATIONEN IM ÜBERBLICK

Grundlegendes Verständnis der Funktionsweise des Internets; Verständnis von Netzwerkprotokollen (TCP/IP) und Netzwerkprogrammierung. Grundlegende Programmierkenntnisse sind empfehlenswert

Administratoren*innen, Analysten*innen, CERT-Mitarbeitende

2 Tage Präsenz

1200,–

Bonn

Veranstaltet durch

Fraunhofer FKIE

Referent:

Daniel Plohmann,
IT-Sicherheitsforscher,
Fraunhofer FKIE

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/grundl-schadsoftwareanalyse-windows