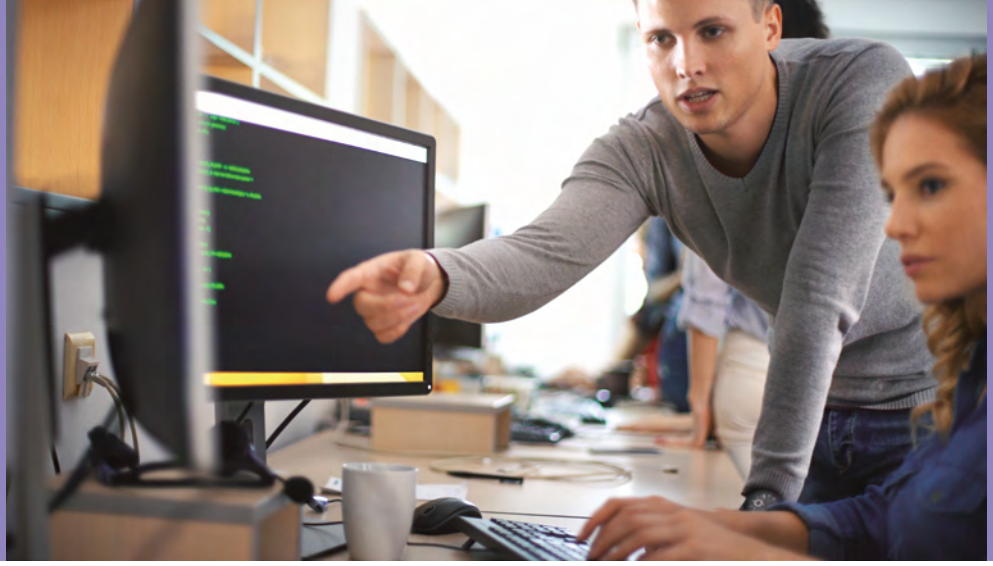

PRÄSENZ

VERSCHLEIERUNGSTECHNIKEN ERKENNEN UND AUFLÖSEN

# FORTGESCHRITTENE SCHAD-SOFTWAREANALYSE WINDOWS

**Moderne Schadsoftware versucht, ihre Analyse durch die Verwendung von verschleiernden Techniken hinauszuzögern.** Dynamisches Entpacken von Code, Verschlüsselung von Strings und Code-Injektionen sind nur einige der genutzten Techniken. Diese Techniken zielen sowohl auf die dynamische als auch auf die statische Analyse ab. Sofern die Detailanalyse einer bestimmten Schadsoftware angestrebt wird, muss ein Schadsoftwareanalyst in der Lage sein, diese Techniken zu identifizieren und anschließend zu entschleiern, damit eine Schadsoftwareanalyse überhaupt möglich ist.

## Inhalte des Seminars

**Manuelles Entpacken von Programmen mit anschließender IAT-Rekonstruktion**

**Manuelles Entpacken von schadsoftwarespezifischen Packern**

**Härten einer virtuellen Maschine**

**Erkennung und Umgehung von Code-Injektionen**

**Automatisierung von IDA Pro mittels IDAPython und Sark**

**Erkennung und Umgehung von Stringverschlüsselung**

**Erkennung und Umgehung von API-Verschleierung**

## Ihr Nutzen

» Nach dem Seminar können Sie Verschleierungsmethoden erkennen und bewerten.
» Sie können einfache Verschleierungsmethoden selbst programmatisch auflösen.
» Anhand vieler praxisnaher Übungen mit aktueller und relevanter Schadsoftware lernen Sie Techniken zu Erkennung und Auflösen von Verschleierungsmethoden kennen.

## INFORMATIONEN IM ÜBERBLICK

Theoretische und praktische Kenntnisse in der Analyse von Windows-Schadsoftware sowie Netzwerkkenntnisse; Umgang mit Windows/ Linux; Umgang mit IDA Pro und Debugger (z. B. x64dbg); Verständnis von x86-Assembler; Programmierkenntnisse in Python (C/C+ vorteilhaft)

Administratoren*innen, Analysten*innen, CERT-Mitarbeitende

2 Tage Präsenz

1200,–

Bonn

Veranstaltet durch

Fraunhofer FKIE

Referent:

Niklas Bergmann,
IT-Sicherheitsforscher,
Fraunhofer FKIE

Weitere Infos und aktuelle Termine buchen unter:

**www.cybersicherheit.fraunhofer.de/fortgeschrittene-schadsoftwareanalyse-windows**