

Grundlagen Schadsoftwareanalyse Windows

Malware untersuchen und verstehen lernen

Lernen Sie, Windows-Schadsoftware zu analysieren und zu verstehen. Mit Tools wie Debugger und IDA Pro vertiefen Sie praxisnah Ihr Wissen über Angriffsvektoren. Das Seminar vermittelt fundierte Techniken zur Erkennung und Analyse und richtet sich an IT-Admins, Analysten und CERT-Mitarbeitende.

Fundierte Einführung in die Analyse von Windows-Schadsoftware

Das Seminar »Grundlagen Schadsoftwareanalyse Windows« bietet eine fundierte Einführung in die Analyse von Windows-Malware.

Teilnehmende lernen, Angriffsvektoren besser einzuschätzen und eigenständig Analysen durchzuführen, um ein grundlegendes Verständnis der Schadsoftware zu erlangen. Dabei werden typische Analyse-Tools wie Debugger

und IDA Pro praxisnah angewendet. Ein zentrales Element des Seminars ist die Vermittlung von Grundkenntnissen zur Detailanalyse von Windows-Schadsoftware.

Sie erhalten eine Einführung in praxisrelevante Analysemethoden und haben die Möglichkeit, sich direkt mit Fachexperten auszutauschen.

Kursdetails auf einen Blick

- Für **Analyst*innen, Admins, und CERTs-Mitarbeiter**
- **Inhouse Training**
- Dauer: **4 Tage**
- Format: **Präsenz**
- Kosten: 2.400,00 Euro (USt.-befreit gem. § 4 Nr. 22a UStG)

Zielgruppe und Nutzen des Seminars im Umgang mit moderner Schadsoftware

Das Seminar richtet sich an eine breite Zielgruppe von IT-Fachkräften, darunter Administratoren, Analysten sowie Mitarbeiterinnen und Mitarbeiter von CERTs, Behörden, Forschungsinstituten und Unternehmen. Es ist damit sowohl für Praktiker aus dem operativen Umfeld als auch für Personen mit analytischem oder forschungsorientiertem Schwerpunkt geeignet.

Für eine erfolgreiche Teilnahme wird ein grundlegendes Verständnis der Funktionsweise des Internets empfohlen, insbesondere in Bezug auf Netzwerkprotokolle wie TCP/IP sowie Kenntnisse in der Netzwerkprogrammierung. Ebenso sollten grundlegende Programmierkenntnisse vorhanden sein, um die vermittelten Inhalte sicher nachvollziehen und praktisch anwenden zu können.

Durch die Teilnahme am Seminar erwerben die Teilnehmenden die Fähigkeit, Schadsoftware zu erkennen und Analysetechniken anzuwenden, um so besser auf die Herausforderungen moderner Cyberangriffe vorbereitet zu sein.

Nach dem Seminar können Sie:

- **Aktuelle Schadsoftware** und ihre Verbreitungswege **kennen**.
- **Systemaufrufe** und **Netzwerkprogrammierung** in Assembler erkennen und **analysieren**.
- **Methoden und Werkzeuge** zur statischen und dynamischen Analyse von Windows-Schadsoftware **anwenden**.

Alle Kursdetails und die Anmeldung finden Sie hier:



<https://s.fhg.de/Windows-Malware>

Kursinhalte

Das Spektrum der behandelten Themen umfasst:

Grundkenntnisse zur Detailanalyse von Windows-Malware

- 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 Assembler
- Einführung in dynamische und statische Analysetechniken mit der Gelegenheit, diese an relevanten Beispielen aktueller Schadsoftware in unserer Laborumgebung zu vertiefen.

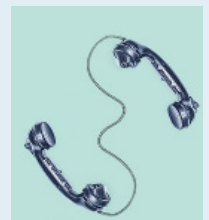
Zugangsvoraussetzung:

Grundlegendes Verständnis der Funktionsweise des Internets, insbesondere Verständnis von Netzwerkprotokollen (TCP/IP) und Netzwerkprogrammierung. Grundlegende Programmierkenntnisse empfohlen.

Fachlicher Ansprechpartner am Fraunhofer FKIE

Dr. Daniel Plohmann
Tel. +49 228 50212-600
daniel.plohmann@fkie.fraunhofer.de

Fraunhofer FKIE
Zanderstraße 5
53177 Bonn



Lernlabor
Cybersicherheit