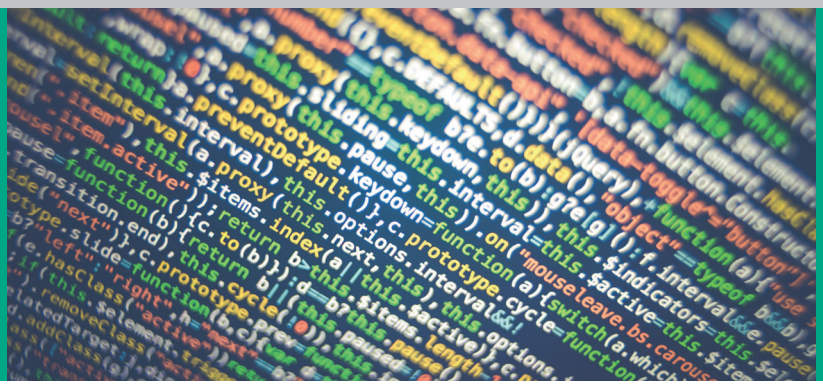
Fraunhofer
ACADEMY

SEMINAR



GRUNDLAGEN SCHADSOFTWAREANALYSE WINDOWS

Malware untersuchen und verstehen lernen

IHRE VORTEILE AUF EINEN BLICK

Nach dem Seminar können Sie…

… Angriffsvektoren von Schadsoftware besser einschätzen.

… Analysen durchführen, um einen grundsätzlichen Eindruck von Schadsoftware zu erhalten.

… typische Analyse-Tools wie Debugger und IDA Pro anwenden.

Dieses Seminar bietet Ihnen…

… eine Einführung in praxisrelevante Analysemethoden für Schadsoftware.

… direkten Austausch mit Fachexperten.

Melden Sie sich gleich an!
www.academy.fraunhofer.de/schadsoftwareanalyse-windows

Die typische Fragestellung: Welche Schadsoftware ist das und was ist ihre Funktionalität?

Oft ist es nicht mehr ausreichend, nur festzustellen, ob sich ein Programm potentiell bösartig verhält oder nicht. Gerade wenn es darum geht, Vorfälle umfassender beurteilen und Schadenspotentiale abschätzen zu können, führt selten ein Weg an aufwendigen, detaillierten Analysen vorbei.

Allein die exakte Bestimmung einer Schadsoftware-Familie kann bereits eine Herausforderung sein, denn Schadsoftware liegt üblicherweise nur als fertig kompiliertes Programm im Maschinencode vor. Da nun also der Quelltext nicht verfügbar ist, sind schnell Spezialwissen wie auch besondere Werkzeuge erforderlich, um Erkenntnisse über Fähigkeiten und Verhalten der Schadsoftware zu erarbeiten.

Unser Angebot: Ein Einstieg in die Schadsoftwareanalyse unter Windows

Im Rahmen des hier angebotenen Seminars sollen deswegen Grundkenntnisse der Detailanalyse von Windows-Malware vermittelt werden. Dabei werden die Grundlagen zu elektronischen Angriffen, ihrer Analyse und Aufklärung sowie innovative Techniken behandelt, um Cyber-Angriffe erfolgreich zu erkennen und zu untersuchen.

INFORMATIONEN IM ÜBERBLICK

Kurs: Grundlagen Schadsoftwareanalyse Windows
Empfohlen sind: grundlegendes Verständnis der Funktionsweise des Internets, insbesondere Verständnis von Netzwerkprotokollen (TCP/IP) und Netzwerkprogrammierung. Grundlegende Programmierkenntnisse empfohlen.
Dauer: 3 Tage in Präsenz
Kurssprache: Deutsch
Teilnehmerzahl: max. 12 Teilnehmer
Veranstaltungsort: Fraunhofer FKIE in Bonn
Kosten: 1.800 €

Veranstaltet durch:

Fraunhofer FKIE

Die Inhalte: Grundkenntnisse zur Detailanalyse von Windows-Schadsoftware

Tag 1
- Einrichtung von und Umgang mit einer Laborumgebung für Schadsoftwareanalysen
- Übersicht Reverse-Engineering und Anwendung von Blackboxing

Tag 2
- Einführung in Assembler und statische Detailanalyse mit IDA Pro
- Gemeinsame praktische Übung von statischer Analyse an realer Schadsoftware

Tag 3
- Vorstellung von Werkzeugen für dynamische Detailanalyse (Debugging)
- Gemeinsame praktische Anwendung aller gelernten Methoden an realer Schadsoftware

Die Lernziele: Schadsoftware kennen und Analysentechniken anwenden

- 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

Die Zielgruppe: Admins, Analysten und CERT-Mitarbeiter

Das Seminar richtet sich an IT-Administratoren, Analysten sowie Mitarbeiterinnen und Mitarbeiter von CERT, von Behörden, Forschungsinstituten und Unternehmen.

UNSERE REFERENTEN

Daniel Plohmann
Sicherheitsforscher in der Arbeitsgruppe Cyber Analysis & Defense des Fraunhofer FKIE

Das Lernlabor Cybersicherheit: Weiterbildung für die IT-Sicherheitsexperten von morgen

Das Lernlabor Cybersicherheit ist eine Zusammenarbeit zwischen Fraunhofer und ausgewählten Fachhochschulen, um aktuelle Erkenntnisse auf dem Gebiet der Cybersicherheit in Weiterbildungsangebote für Unternehmen zu überführen. Fach- und Führungskräfte aus Industrie und öffentlicher Verwaltung erhalten an zahlreichen Standorten in Deutschland eine kompakte Qualifizierung in hochwertigen Laboren mit aktueller IT-Infrastruktur.

HABEN SIE NOCH FRAGEN ZU…

… Schadsoftware und Analysetechniken?

Daniel Plohmann | Fraunhofer FKIE
Telefon +49 228 50212600
daniel.plohmann@fkie.fraunhofer.de

… Anmeldung, Organisation oder weiteren Angeboten?

Adem Salgin | Fraunhofer Academy
Telefon +49 89 1205-1555
cybersicherheit@fraunhofer.de