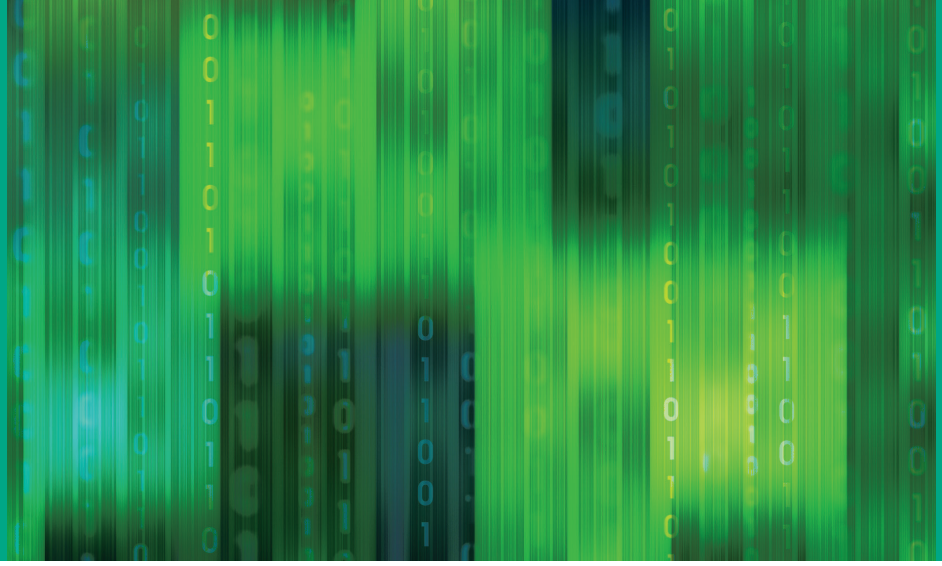

INFORMATIONEN IM ÜBERBLICK

Kurs: Fortgeschrittene Schadsoftware-analyse Windows

Voraussetzungen:

– Theoretische und praktische Kenntnisse in der Analyse von Windows-Schad-software (siehe Modul »Grundlagen Schadsoftwareanalyse für Windows«)
– Umgang mit Windows/Linux
– Umgang mit IDA Pro und Debugger (z. B. x64dbg)
– Netzwerkkenntnisse
– Programmierkenntnisse in Python (wichtig) sowie C/C++ (vorteilhaft)
– Verständnis von x86-Assembler

Dauer: 2 Tage in Präsenz

Kurssprache: Deutsch

Teilnehmerzahl: max. 12 Personen

Veranstaltungsort: Fraunhofer FKIE in Bonn

Termin: 14.-15.11.2018, 21.-22.05.2019, 8.-9.10.2019

Kosten: 1200 €

Veranstaltet durch:

Fraunhofer FKIE

WEITERE SEMINARE AUS DIESEM BEREICH

Sie interessieren sich zunächst für eine Einführung zur Analyse von Windows-Schadsoftware? Dann sehen Sie sich doch unseren Basic-Kurs »Grundlagen Schadsoftwareanalyse Windows« an: **www.academy.fraunhofer.de/schadsoftwareanalyse-windows**

Die Inhalte

Tag 1

– Manuelles Entpacken von Schadsoftware, Rekonstruktion von API-Importen
– Methoden zur Erkennung und Abhärtung von Analyseumgebungen
– Code-Injektionen in Schadsoftware (CreateRemoteThread und Process Hollowing) sowie Techniken zur Analyse

Tag 2

– Automatisierung von IDA Pro mittels IDAPython
– Deobfuskierung von Stringverschlüsselung
– Deobfuskierung von API-Obfuskierung
– Diskussion und Austausch

Die Lernziele

Kennen

– Gängige Verschleierungsmethoden wie String-Verschlüsselung, API-Verschleierung, Code-Injektionen
– Möglichkeiten und Grenzen der Entschleierung

Verstehen

– Applikationspacker, Code-Injektionen, API/String-Verschleierung

Die Zielgruppe

Angehende Schadsoftwareanalysten, die bereits erste Erfahrungen mit dynamischer und statischer Analyse haben

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?

Thomas Barabosch | Fraunhofer FKIE
thomas.barabosch@fkie.fraunhofer.de

… Anmeldung, Organisation oder weiteren Angeboten?

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

UNSER REFERENT

Thomas Barabosch
Wissenschaftlicher Mitarbeiter bei Fraunhofer FKIE