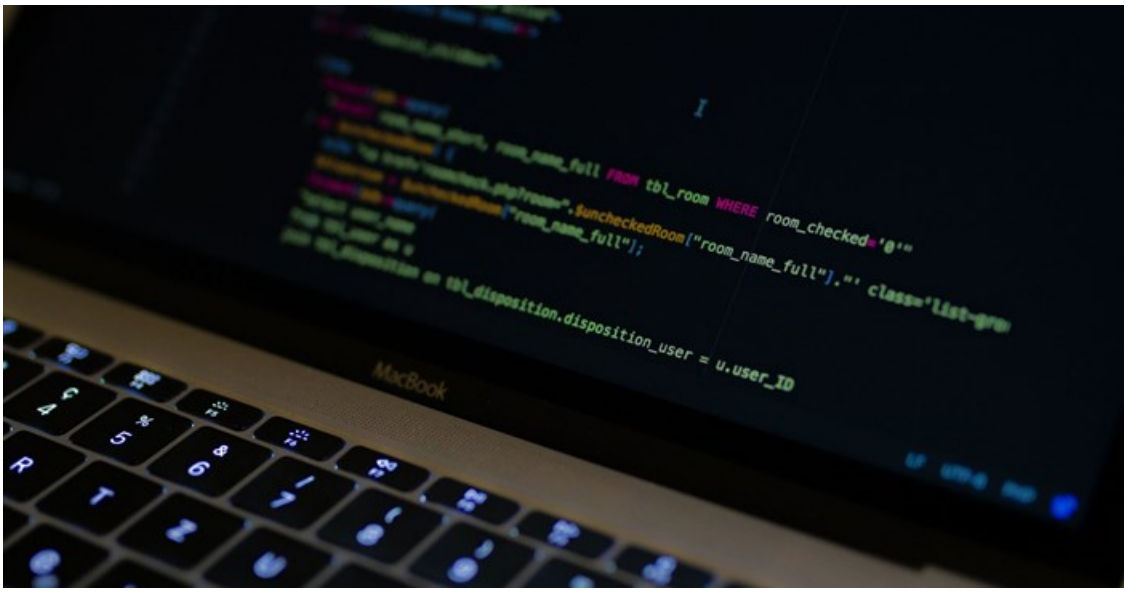
Codebreakers reveals reverse engineering is toughest cybersecurity task

Cyber security specialists often need to do a detailed examination of a software product or web application to detect vulnerabilities or hidden features, working from the outside in. That's called reverse engineering and it covers a broad range of areas, including decompiling and disassembling executable files and libraries, and analysis of system data.



Coding SQL Query in a PHP file using Atom. Source: Caspar Camille Rubin/Unsplash

According to the external research, the vast majority of cyber professionals state that the cybersecurity skills shortage and skills gap have not improved over the past few years and even got worse. To help InfoSec practitioners enhance their skills, Kaspersky has been continuously running expert trainings both online and offline, organising bootcamps and workshops.

In June 2023, Kaspersky conducted the Codebreakers cybersecurity competition with over 550 participants from 35 countries including France, Germany, USA, Brazil, China, India, UAE, Saudi Arabia, Turkey, South Africa, and others. It was designed to test different hard skills of InfoSec professionals in a limited timeframe and reveal strengths and weaknesses in their expertise.

Experts from Kaspersky Global Research and Analysis Team (GReAT) set a number of cybersecurity challenges in three different tracks: Threat Hunting with Yara, Reverse Engineering, and Incident Response.

Participants were given such tasks as analysing an attack scenario on a corporate network and collecting evidence; writing

Yara rules for detecting malware; reverse engineering a program and uncovering its secrets by cracking the APK obfuscator; training a machine learning model.

Only 18 participants were able to solve all the tasks. The best results were shown by InfoSec practitioners from the Czech Republic and South Korea.

Most InfoSec professionals are fine with Yara

According to the competition results, the tasks that were most complicated for the participants were related to reverse engineering as they required specific knowledge of system programming, features of x86 and ARM architecture and practical skills in working with disassemblers (e.g., IDA Pro, Ghidra) and debuggers (e.g., x64dbg/WinDBG/OllyDbg).

The tasks that were solved fastest were associated with Yara, one of the most familiar and popular tools among those that analyse malicious code. These tasks were the easiest to perform.

“We tried to make the CTF tasks as close as possible to the real-world challenges InfoSec professionals face every day. Participants were required to apply their knowledge in a variety of situations, ranging from beginner-friendly to expert level, testing their readiness to deal with advanced cyber threats in future scenarios. Congratulations to the finalists who managed to solve all challenges and I am confident they will fully benefit from the free training offered by Kaspersky,” says Dan Demeter, senior security researcher at Kaspersky.

Why defending against hackers is an uphill battle

26 Jun 2023

“We are trying to keep up with the times and contribute to better professional background of InfoSec practitioners. Our expert training portfolio provides courses covering different cybersecurity topics, from basic knowledge in reverse engineering and writing Yara rules to advanced methods of finding threats and malware analysis,” comments Yuliya Dashchenko, team lead of expert trainings at Kaspersky.

“We believe that our cybersecurity competition will help participants to reveal and work on the areas that need improvements to be able to cope with even the most complex threats in the future.”

The winner of Codebreakers received free access to one of Kaspersky’s Expert Trainings. Others were given a big discount for training programs.

“I enjoyed that the competition was well balanced and contained good challenges. I loved the scoring system as well and was happy to play with Klara,” says one of the participants under the nickname Termopan.