Digital Single Market

Projects news and results6 December 2012

SysSec Research wins Gold Prize at IWSEC Malware Analysis Competition

On 7-8 November 2012, the team of Athanasios Petsas, Zacharias Tzermias, and Nikolaos Tsikoudis, from FORTH (SysSec Project Coordinator) won the Gold Prize at the malware competition analysis of the International Workshop on Security (IWSEC) Cup 2012.

[1]

The winning team, nicknamed Minotaurus, after the mythical half-bull/half-human creature from Crete which lived in the Minoan Labyrinth of Knossos, competed against two teams from Japan and one team from the USA. All the teams competed in three challenges involving, traffic analysis, malicious PDF analysis, and Android application analysis. To reach the winning prize, Minotaurus made extensive use of **MDScan:** a tool developed, in part, in the context of the **SysSec Network of Excellence.** MDSan is being used to detect polymorphic malicious attacks masquerading themselves as ordinary data hidden inside PDF files. Although PDF files are usually perceived as innocent “data” files, they may actually contain executable code that can pose a significant threat to anyone opening it. Despite the best efforts from several available PDF/ativirus tools, malicious PDF files remain a sizeable threat that may go undetected, especially when aggressors obfuscate their code in order to conceal it further. MDScan takes this into

account and, by using a combination of different analysis techniques, tries to uncover and expose the obfuscated executable code and raise an alert before the malicious code manages to compromise the computer.

Read full text [2]
Contact
meltini@ics.forth.gr [3]
Share this page

Links
[1] https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/newsroom/syssec_winning_team_3810.jpg
[2] http://www.syssec-project.eu/news/2012/11/23/forth-gold-prize-iwsec12/
[3] mailto:meltini@ics.forth.gr