Title:
Fileless attacks – PowerShell-based techniques

Abstract:
Introduction of PowerShell utility in Windows was the beginning of a new series of cyber-attacks that leverage scripting languages and several obfuscation techniques with the fact that security products were at that time designed to skip system based tools from scanning. While fileless techniques were known for some time, they were never prevalent up to the moment PowerShell has become a part of all modern Windows OSs. These attack techniques are based on the usage of command line options available on PowerShell utility that allows for code execution without usage of a file that contain the actual code.

This talk will present how these types of attacks have evolved in terms of both features (from simple downloaders to OS loaders capabilities that can execute an entire binary in memory) and obfuscation techniques. The final part of this talk will present some ideas that can generally be used to identify such cases and are not limited to one scripting language.

Short Bio:
Dragoș Gavriluț is the director of Cyber Threat Intelligence Lab at Bitdefender, managing a team of 120+ people that develops heuristic detections, cloud-based services, system testing services, disinfection routines, Android and iOS analysis, event correlation algorithms, data mining, IoT and cybersecurity analysis. He is also an associate professor at the Alexandru Ioan Cuza University of Iași, where he received his Ph.D. in 2012, with the thesis entitled “Meta-heurisics for Anti-Malware Systems”. He received his B.Sc. and M.Sc. in computer science from the same university, in 2004 and 2006, respectively.