17 January 2019

Identifying and Defeating Modern Malware Code Obfuscation (1:10-1:50 pm ET)

Mark your calendars and come join your friends in the CAE community for a Tech Talk. CAE Tech Talks are free and conducted live in real-time over the Internet so no travel is required. You can attend from just about anywhere (office, home, etc.) Capitol Technology University (CTU) hosts the presentations using their online delivery platform (Adobe Connect) which employs slides, VOIP, and chat for live interaction. Just log in as "Guest" and enjoy the presentation(s).

Date: Thursday, 17 January 2019

Time: 1:10-1:50 pm ET

Location: https://capitol.adobeconnect.com/cae_tech_talk/

Just log in as "Guest" and enter your name. No password required.

Title/Topic: Identifying and Defeating Modern Malware Code Obfuscation

Audience Skill Level: Intermediate

Presenter(s): Dr. Josh Stroschein – Dakota State University

Description:

Modern malware uses a wide variety of code obfuscation techniques to hide it's true intentions and to avoid detection. In this talk, we'll explore the latest in native code obfuscation techniques as well as a few techniques commonly used with interpreted languages. We will spend time discussing such methods as dynamically constructing import tables, hiding and using shellcode, packing, string obfuscation, use of virtual machines and other anti-analysis techniques. We'll dig deep into the techniques by examining a wide variety of malware, including those used by nation-states. By the end of this talk you'll have a technical understanding of how they work and how to defeat them!

CAE Tech Talks are recorded; view them here: https://www.caecommunity.org/content/cae-tech-talk-resources

For questions on CAE Tech Talk, please send email to CAETechTalk@nsa.gov