Title: Diving Into Development Of Microsoft Windows Kernel Exploits

Abstract:

Description:

Course Agenda:

First day:

- Setting up the environment
- Basics of Kernel Debugging with Windbg
- Microsoft Kernel Vulnerabilites Overview
- Arbitrary Memory Overwrite Exploitation

Second day:

- Pool Overflow/Corruption Exploitation

Third day:

- Various Kernel Exploit Mitigation Technologies Overview
- Hardcore Pool Overflow/Corruption Exploitation

Fourth Day(Advanced topics)

- Kernel attack surface from a sandbox
- Hyper-V
- WoA: Windows on ARM64

Students minimum requirements

Training attendees should be familiar with basic operating system concepts and have hands-on experience using the Windows operating system. Attendees should be familiar with the Win32 API, C (or derived) programming language and have basic knowledge of x86/x86-64 assembly language.

Hardware:

64-bit machine with at least 8GB of RAM (16BG and more is better)

Software:

- IDA Pro
- Visual Studio (at least Visual express c++)
- Virtualization software:VMWare WorkStation

The training covers development of windows kernel exploits for following OS versions: Windows 7, Windows 8, Windows 8.1, and Windows 10 up-to not-yet-released RedStone 6 aka 19H1.

A brief biography of the trainers:
Nikita Tarakanov