1700 - Taking Windows 10 Kernel Exploitation to the next level - Leveraging write-what-where vulnerabilities in Creators Update

Saturday at 17:00 in Track 2
45 minutes | Demo, Exploit
Morten Schenk*Security Advisor, Improsec*

Since the release of Windows 10 and especially in the Anniversary and Creators Updates, Microsoft has continued to introduce exploit mitigations to the Windows kernel. These include full scale KASLR and blocking kernel pointer leaks.

This presentation picks up the mantle and reviews the powerful read and write kernel primitives that can still be leveraged despite the most recent hardening mitigations. The presented techniques include abusing the kernel-mode Window and Bitmap objects, which Microsoft has attempted to lock down several times. Doing so will present a generic approach to leveraging write-what-where vulnerabilities.

A stable and precise kernel exploit must be able to overcome KASLR, most often using kernel driver leaks. I will disclose several previously unknown KASLR bypasses in Windows 10 Creators Update. Obtaining kernel-mode code execution on Windows has become more difficult with the randomization of Page Table entries. I will show how a generic de-randomization of the Page Table entries can be performed through dynamic reverse engineering. Additionally, I will present an entirely different method which makes the usage of Page Table entries obsolete. This method allocates an arbitrary size piece of executable kernel pool memory and transfers code execution to it through hijacked system calls
Morten Schenk
Morten Schenk (@blomster81) is a security advisor and researcher at Improsec ApS, with a background in penetration testing, red teaming and exploit development. Having a high craving for learning and torture based on taking certifications like OSCP, OSCE and OSEE, Morten's research is specifically focused on binary exploitation and mitigation bypasses on Windows. He blogs about his research at https://improsec.com/blog/

@Blomster81

#defcon25/by_track/track2/saturday #defcon25/By_Day/_saturday