InvisiMole (Malware Family)

By Fraunhofer FKIE

InvisiMole had a modular architecture, starting with a wrapper DLL, and performing its activities using two other modules that were embedded in its resources, named RC2FM and RC2CL. They were feature-rich backdoors and turned the affected computer into a video camera, letting the attackers to spy the victim.
The malicious actors behind this malware were active at least since 2013 in highly targeted campaigns with only a few dozen compromised computers in Ukraine and Russia. The wrapper DLL posed as a legitimate mpr.dll library and was placed in the same folder as explorer.exe, which made it being loaded during the Windows startup into the Windows Explorer process instead of the legitimate library.
Malware came in both 32-bit and 64-bit versions, which made this persistence technique functional on both architectures.

The smaller of the modules, RC2FM, contained a backdoor with fifteen supported commands indexed by numbers. The commands could perform simple changes on the system and spying features like capturing sounds, taking screenshots or monitoring all fixed and removable drives.

The second module, RC2CL, offered features for collecting as much data about the infected computer as possible, rather than for making system changes. The module supported up to 84 commands such as file system operations, file execution, registry key manipulation, remote shell activation, wireless network scanning, listing of installed software etc. Though the backdoor was capable of interfering with the system (e.g. to log off a user, terminate a process or shut down the system), it mostly provided passive operations. Whenever possible, it tried to hide its activities by restoring the original file access time or safe-deleting its traces.

▶ [TLP:WHITE] win_invisimole_auto (20251219 | Detects win.invisimole.)
