Anti-Unpacker Tricks 1

Author	Peter Ferrie
Author email	peter.ferrie©gmail.com
Author website	http://pferrie.tripod.com/

Description	Anti-unpacking tricks can come in different forms, depending on what kind of unpacker they want to attack. The unpacker can be in the form of a memory-dumper, a debugger, an emulator, a code-buffer, or a W-X interceptor. It can be a tool in a virtual machine. There are corresponding tricks for each of these, and they will be discussed separately. - A memory-dumper dumps the process memory of the running process, without regard to the code inside it. - A debugger attaches to the process, allowing single-stepping, or the placing of breakpoints at key locations, in order to stop execution at the right place. The process can then be dumped with more precision than a memory-dumper alone. - An emulator, as used within this paper, is a purely software-based environment, most commonly used by anti-malware software. It places the file to execute inside the environment and watches the execution for particular events of interest. - A code-buffer is similar to, but different from, a debugger. It also attaches to a process, but instead of executing instructions in-place, it copies each instruction into a private buffer and executes it from there. It allows fine- grained control over execution as a result. It is also more transparent than a debugger, and faster than an emulator. - A W-X interceptor uses page-level tricks to watch for write-then-execute sequences. Typically, an executable region is marked as read-only and executable, and everything else is marked as read-only and non-executable (or simply non-present, depending on the hardware capabilities). Then the code is allowed to execute freely. The interceptor intercepts exceptions that are triggered by writes to read-only pages, or execution from non-executable or non-present pages. If the hardware supports it, a read-only page will be replaced by a writable but non-executable page, and the write will be allowed to continue. Otherwise, the single-step exception will be used to allow the write to complete, after which the page will be restored to its non-present state. In either case, the page address is kept in a list. In the event of exceptions triggered by execution of non-executable or non-present pages, the page address is compared to the entries in that list. A match indicates the execution of newly-written code, and is a possible host entrypoint.
Image	no image available
Filesize	314 kB

Date	Wednesday 07 May 2008 - 04:28:30
Downloads	2963
Download