"1469" kernelcaches

Another class of kernelcaches are 1469 kernelcaches, so-named by the Author due to a mistake in their build process, leaving the KernelCacheBuilder's `RC_ProjectSourceVersion` environment setting so that it is incorrectly embedded in XNU's own `LC_SOURCE_VERSION`. These kernels have first appeared in iPhone 12 betas for the iPhone7,x (i.e. 6S) and iPad4,x series, but have since been adopted by the iPhone11,x as well. It is reasonable to believe that this format will be the preferred one by Apple going forward.

XNU's compilation process and the kernelcache creation is substantially different in these kernelcaches:

- The kernelcache segmentation is altered to add `__PPL*` segments, containing PMAP management code which is protected by KTRR (presumably to avoid clever bypasses such as that of Luca Todesco in the Yalu 10.2 jailbreak (III/24), and the TrustCache injection method exposed (and, effectively, killed) by @Xerub (III/25)). These segments include `__PPLDATA[_CONST]` and `__PPLTEXT` (similar to their regular counterparts) and a `__PPLTRAMP` containing trampolines pointers initialized at runtime.
- The `__PRELINK_[TEXT/EXEC/DATA]` segments and various `PLK_*` segments (`PLK_[LINKEDIT/LLVM_COV/DATA[_CONST]`) are defined, but are not mapped to the file, meaning they might as well be removed.
- Other existing segments are resectioned: `__TEXT` now contains `__fips_hmacs`, `__ustring` and an embedded `__info_plist`, and the `__TEXT_EXEC` contains an `initcode` section. The various `__llvm*` sections (which weren't mapped anyway) are removed from `__DATA`. Also in `__DATA` are two new sections, but only on A12 devices - `fwFirmwareImage` (containing the A12's PMP firmware) and `__auth_ptr` (enabling ARMv8.3 PAC). `__KLD` similarly defines `__auth_ptr` for PAC.

- The `__PRELINK_INFO.__info` section size is significantly reduced, with the `_PrelinkLinkKASLROffsets` and `_PrelinkLinkKCID` keys removed. Further, the `PrelinkExecutableLoadAddress` of all the kexts has been removed as well, making this dictionary far less useful for reversing the kernel structure
- In place of the missing extension load address keys, `__PRELINK_INFO` now contains two additional sections - `__PRELINK_INFO.__kmod_info` and `...__kmod_info`. The first provides a list of `struct kmod_info` structures (discussed later in this chapter), and the second an address list of the extensions' Mach-O Headers. The headers, however, now only contain a single segment, `__TEXT_EXEC.__text`, with their strings and other data mixed with those of other kexts, and the kernel proper.
- All pointers have been converted to a special tagged notation (in their top and otherwise unnecessary 24-bits), and in some cases (e.g. the `sysent` and `mach_trap_table` entries) replaced by tagged offsets relative to the kernel base load address. Brandon Azad [was the first to document this publicly document this][batp].

Those readers lamenting the loss of symbols can draw solace from that the `joker` tool has been revised to work with 1469 kernelcaches. As a farewell present for developers Apple left in the 12β1 kernels not just the regular set of some 4,800 or so exported symbols - but over 85,000(!) of them - including static, unexported, and kext internal symbols. This was a true boon, and `joker` now recognizes many more important symbols in all kernels, 1469 and other. Kextraction from 1469 kernels is (at least presently) not supported due to the dissolution of non-code segments, but `jtool2` can operate on the kexts without needing to remove them from the kernelcache first.