Full SWEEP vs. Quick SWEEP

Dr. Jan Hruska, Sophos Plc, Oxford, England

Part # tr000012/950101

From SWEEP version 2.61 Quick sweep is enabled by default.

The difference between Full and Quick sweep is that the Full sweep searches for 24-byte patterns in **every part** of every executable file as well as doing a Quick sweep, while Quick sweep looks for a precise match at the **entry point** in every executable file. Quick sweep has an algorithmic search capability which is used to search for polymorphic viruses. A typical example of such an algorithm could be: check for 12th byte from entry point for being 6a hex, then take the following byte, use it as an offset and check that that location contains a byte between a7 and a9.

Since Full sweep looks for fixed patterns in addition to using an algorithmic search for polymorphic viruses, it has a somewhat increased chance of discovering mutated (intentionally modified) non-polymorphic viruses. For example:

```
ab76 8928 9304 1262 13..   Virus 1
90ab 7689 2893 0412 62..   Virus 2
```

Virus 2 is a slightly modified version of Virus 1 with the pattern ab76 8928 9304 1262 13 shifted right by one byte. If one looks for precisely that pattern in precisely that position Virus 2 is not going to be discovered. The more loose byte-by-byte search will, of course, discover it.

Current Quick sweep detects all known viruses (about 4000) except 2 (about 2% of Mutation Engine samples) and Commander Bomber. These 2 viruses have never been reported in the wild.

Our recommendation is to use the default, Quick sweep from now on, as it provides excellent detection capability while executing about 5 times as fast as the Full sweep. This also means that the software is more likely to be used.

Should the virus situation change in the future in such a way that Full sweep again becomes necessary, the default mode may change.

The -Q and -F command line qualifiers specify the Quick and Full sweeping, respectively. For example

```
SWEEP -F C:
```

performs a Full sweep of drive C regardless of the default setting.

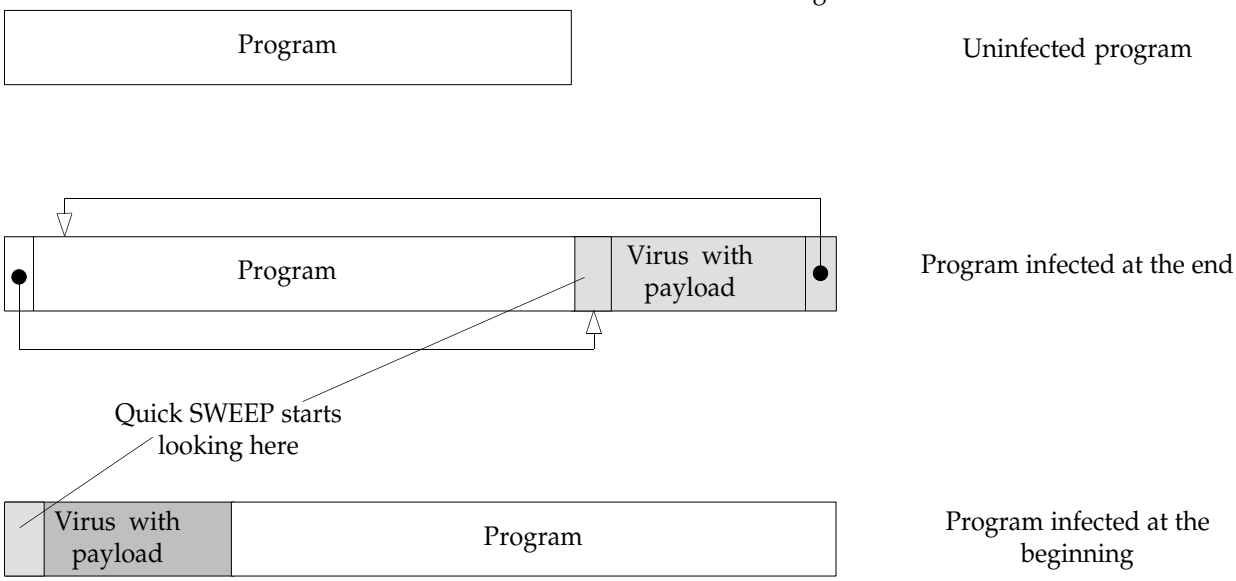

Fig. 1 - Program infection with a parasitic virus: Quick sweep