Frankenstein: The Modern (Virus) Prometheus

Written by Marco Attard
23 August 2012

We all know the Frankenstein story, right? A genius scientist creates a man out of a selection of body parts, before bringing it to life. Now University of Texas research create something similar to the good doctor-- with computer malware.

Called (what else?) Frankenstein, the self-camouflaging malware copies pieces of code performing specific tasks (aka gadgets) from regular programs before "stiching" them into working malware code. Semantic blueprints point Frankenstein to the gadgets ideal for its purposes.

Whenever it infects a new computer, Frankenstein repeats swaps with different (if similar) gadgets. It also adapts to look like regular software-- making it difficult for antivirus software relying on specific malware signatures to detect.

First presented at the USENIX Workshop on Offensive Technologies, in its current form Frankenstein build 2 simple malware algorithms out of gadgets.

"The 2 test algorithms we chose are simpler than full malware, but they are representative of the sort of core logic that real malware uses to unpack itself," comments researcher Kevin Hamlen. "We consider this a strong indication that this could be scaled up to full malware."

The only "problem" (if you can call it that) Frankenstein has is the kind of blueprint it employs--

too specific leaves the malware with little choice of gadgets to hunt down (making it easier to detect), while too loose is too vague for Frankenstein to follow. For now, anyway.

The researchers believe Frankenstein can be a powerful "active defense" tool... or rather, a weapon to infiltrate enemy computer systems with. Hope it doesn't make it to the wilds outside military efforts (the US air force part-sponsored the research), then.

Go Frankenstein: Stitching Malware from Benign Binaries

Go Frankenstein Virus Creates Malware by Pilfering Code (New Scientist)