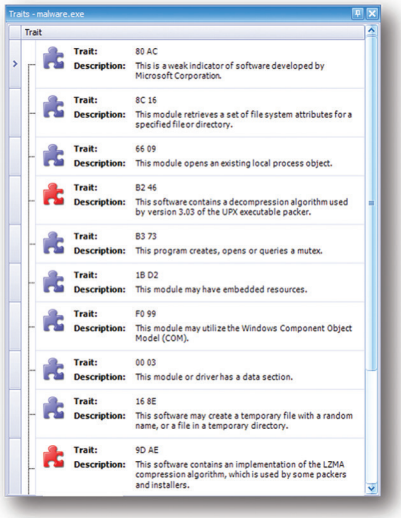

CounterTack
Digital DNA (DDNA)

Digital DNA (DDNA) analyzes memory to identify potentially malicious behaviors exhibited by processes running on managed computers. It works from the cloud using an embedded agent on the devices you wish to monitor. We downloaded the Responder installer – DDNA uses this installer for Windows – and immediately hit a wall. The licensing options for this product are obscure. For example, we were told to click the Responder icon and follow the demo mode button to receive a license. There was no such button. It turns out that you need to work through the support desk and then everything works.

Documentation for DDNA also is a bit obscure. After pouring through the Responder docs, we finally found the section on DDNA, shown as a tab on the Responder desktop. We assume that this is because DDNA often is considered an OEM product and is integrated into Responder PRO to perform its particular tasks.

All of that said, this really is a useful tool. It approaches threat analysis somewhat differently from other products and we certainly have no quarrel with that. The tool creates what CounterTack refers to as a Digital DNA Sequence. This is a hex sequence that is, presumably, unique to the target of analysis. The sequence – shown in the Sequence column – contains the trait sequence for the target. Taken together, the DDNA trait sequence is able to identify the presence of new or previously unknown malware. That, in our view, is the big benefit here.

Since DDNA works in memory, it is looking at an executed malware and very likely analyzing it – whether the malware uses a packer or crypter or not. It also leads to false positives on occasion. For example, the documentation warns of DRM causing false positives because it behaves the same as some types of malware.

The tool is capable of providing reports, specific traits, binaries, strings and symbols. In short, it behaves very much like a traditional reversing tool or debugger with the benefit that it picks out those things that are of particular interest to analysts.

Once you get this installed, it still is a bit quirky. That said, it has a lot of good information and is a solid memory analysis tool for threat analysis based on solid intelligence. We liked the analysis capabilities and the easy to understand analysis. However, for all of that, analysts with a technical background, particularly in forensics, will find this easiest to work with. Many of the displays will be quite familiar to digital forensic specialists, but most of these displays are at the drill-down level rather than at a top page. The top page view is quite clear, self-explanatory and indicative of what your next drill-down steps should be. In short, this is more of a technical analyst's tool than some tools that take an approach comfortable to lay analysts.

– Peter Stephenson, technology editor

DETAILS

Vendor CounterTack

Price $14,000 per perpetual seat; $7,500 annual subscription seat.

Contact countertack.com

Features	★★★★★
Performance	★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★½

OVERALL RATING ★★★★★

Strengths Good level of detail, relatively easy to use and an excellent price point.

Weaknesses Can be a bit quirky, especially during installation.

Verdict This is a good tool and certainly has a place in your analysis stack.

CounterTack®
100 5th Avenue, First Floor, Waltham, MA 02451
855-893-5429
sales@countertack.com
www.countertack.com