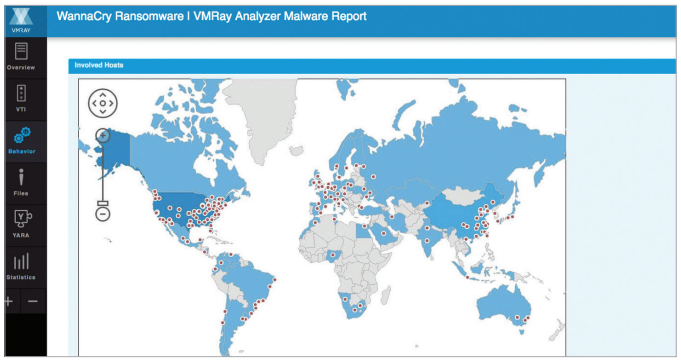

VMRay

VMRay Analyzer

VMRay Analyzer is an automated sandbox with a few additional features that make it a nice stand-alone malware analysis tool. While it is available as an on-premises offering, it is most often used as a cloud service. However, running on-prem offers the additional benefit of being able to use gold images of your own environment as targets. This tool uses the unique approach of depending upon the hypervisor in a virtual environment.

Typically, we think of virtual environments as being susceptible to discovery by the malware sample which, of course, has been written to detect analysis attempts, especially in the virtual. However, in the case of VMRay Analyzer we don't use the typical techniques of agent-based hooking. Instead we see that the malware's behavior is being monitored without direct contact. Targets are available to be infected and the behavior of the malware pre-, post-, and during the infection and payload process is closely monitored.

We used a ransomware sample of an older – relatively speaking – malware: CryptoWall 3.0, hash, ed74b74d02b91b3fbfddc94484f031e0. We tested the sample in VirusTotal to get a baseline of the malware without, of course, the details. The result was that VMRay identified the sample and the analysis gave us a lot of detail. The visualizations range from creative – the addresses and domains that the malware calls out to are geolocated on a map, for example – to very simple tables packed with information. Perhaps an FAQ VMRay uses a process called the VMRay Threat Identifier (VTI). This provides a lot of analysis. VTI operates based upon a set of rules which either can be out of the box or modified/created by the analyst.

Additionally, YARA rules, file and URL reputations and multi-AV scanners. These do the contextual work while the sandboxing/dynamic analysis is left to the proprietary VMRay sandbox. This allows enriched output. As well, there is a REST API that simplifies integration with other systems. Overall, this is a powerful, moderately easy to use, reasonably-priced tool for analysts who don't want to do manual analysis but want the benefit of full information. We found the hypervisor approach to be effective and the tool did not succumb to our sample, rather, it performed a solid analysis, apparently unobserved by the ransomware.

The web site largely is a marketing site. It does, however, have some useful materials and a blog. We would like to see a bit more support-oriented contact, such as a FAQ (which we looked for but were unable to find). The blog is very good, however, and contains a lot of useful information. Support is included but there are optional support packages about which you will need to ask the company. Standard support is 8X5 but includes both email and phone support. This is a German company but it has tier 1 support in its Boston office. We found the company exceptionally responsive to our requests for information.

We liked this product in general, and it certainly is priced attractively. To use it you need some, but not a lot, of prior knowledge about malware analysis so that makes it a perfect tool for the intermediate or senior security engineer just adding malware analysis to his or her tool kit.

– Peter Stephenson, technology editor

DETAILS

Vendor VMRay

Price Starts at $2,700 USD annual subscription for single-user Investigator license

Contact vmray.com

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

OVERALL RATING ★★★★★

Strengths Easy to use with a lot of features – its hypervisor-based agentless approach.

Weaknesses The web site could be a bit more informative.

Verdict Solid malware analysis tool, especially good for engineers just getting started with malware analysis. We make this our Recommended tool for this month.

VMRAY

51 Melcher Street, 7th Floor
Boston, MA 02110
(888) 958-5801
sales@vmray.com
www.vmray.com