Interested in learning more about security?

SANS Institute InfoSec Reading Room

VMRay Analyzer: Rapid Malware Analysis for Incident Response (IR) Teams

In our hands-on testing, we found that VMRay Analyzer's agentless approach to malware analysis is an effective way to provide rapid incident response. VMRay bridges the gap between an easy-to-use interface and back-end technology that provides a novel platform for analyzing advanced threats.

SANS

A SANS Product Review

VMRay Analyzer: Rapid Malware Analysis for Incident Response (IR) Teams

Written by **Matt Bromiley**

March 2018

Sponsored by:

VMRay

Executive Summary

Incident response is no easy gig. Attackers change their tactics just as fast as analysts can learn about them. From tracking lateral movement to uncovering stealthy malware, incident response (IR) teams often find their hands full. These teams need the resources that allow them to move quickly and make actionable decisions to protect the organization.

Many IR teams maintain a wide range of skills, but despite best efforts, they cannot always maintain the full roster they *want*, which may leave a gap in capabilities. One of the most common capabilities organizations look to support is malware analysis. Data gathered from effective malware analysis can help in detection, containment and remediation efforts.

Despite the benefits that malware analysis provides, many teams have concerns about executing malware, even in so-called safe systems. Thus, they are often seeking tools that integrate with the current workflows while enhancing the team's knowledge of malware and threats.

In this product review, we examined VMRay Analyzer, an agentless, hypervisor-based malware analysis platform. Specifically, we looked at:

- The product's ease of use
- The tool's malware analysis capabilities, including the benefits of agentless analysis

- How the tool lends itself to easy integration and adoption
- How VMRay can increase your incident response team's capabilities and overall effectiveness

Overall, we enjoyed VMRay Analyzer. We found the GUI intuitive, easy to use and designed around an analyst's thought processes. The tool has the ability to smoothly integrate with any workflow and assist teams in effective malware analysis. VMRay Analyzer expertly handles multiple types of malware samples, ranging from malicious documents to executables and Java archives. The most impressive and notable feature is the lack of an agent for monitoring malware activities. Agentless analysis sets VMRay Analyzer apart from other tools currently available.

All of these features make VMRay Analyzer a robust malware-analysis tool that would be a plus to any team's investigative arsenal.

Defeating Barriers to Adoption

One of the most common issues that many incident responders encounter when incorporating a tool into their workflow is ease of use versus analytical capabilities. How they are balanced can determine whether an organization fully adopts a tool. Many tools are designed with impressive behind-the-scenes analytics but have horrible user interaction; poorly designed user interfaces that make data consumption difficult won't be useful to teams. On the other hand, tools that have an extreme focus on a user-friendly, intuitive GUI but are weak on back-end analytics fail to deliver the technical chops that incident responders desire.

While it may seem superficial to judge the quality of a tool based on appearance, keep in mind that products are often tested or previewed by senior analysts and key decision makers but used by the senior analysts plus the junior analysts who support them. Striking a balance between ease of use and technical delivery helps the senior analysts focus on teaching the concepts of incident response, not the concepts of one tool.

Happily, VMRay has struck that balance.

Upon accessing VMRay Analyzer, the first two things to greet the analyst are a submission box adjacent to severity statistics of recently submitted malware samples. See Figure 1.

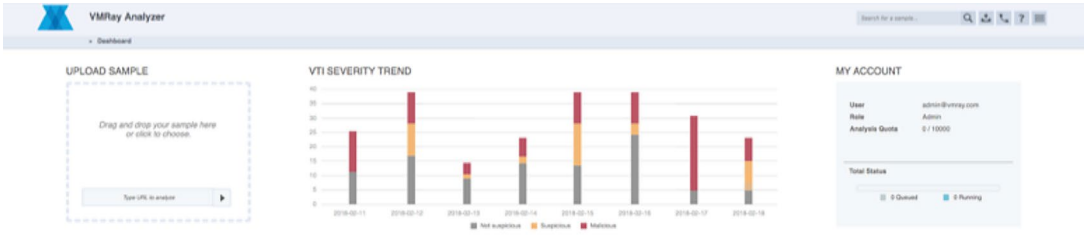

Figure 1. VMRay Analyzer Dashboard

Malware submission can be done via simple drag-and-drop, or via folder searching if you click in. There are also API functions, which we will discuss later. Note that in our testing, we uploaded only about a dozen samples, but in a production, investigative environment, one could easily expect this to reach hundreds, if not thousands, of samples daily.

One feature we like about making malware submission a main focus of the analyst dashboard is that it encourages submissions. Too often, teams have unique or decentralized methods of handling malware, which leads to compartmentalization of case knowledge that could benefit others. Malware analysis helps organizations tie attacks together and understand how attackers modify their techniques. By establishing an easy mechanism through which analysts can submit, our experience has shown that more will submit.

The dashboard of VMRay Analyzer is straightforward and analyst-focused. Directly below the contents shown in Figure 1, VMRay Analyzer displays data points for recently uploaded samples, including the filename, what type of file was uploaded and whether or not the sample received a severity rating. Figure 2 provides more detail of the "Submissions" section of the VMRay Analyzer Dashboard.

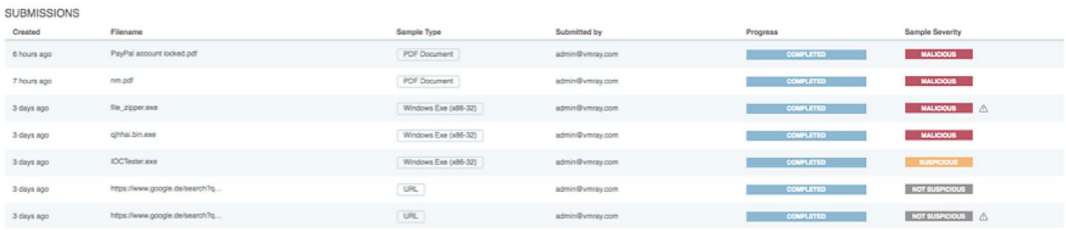

Figure 2. "Submissions" Section of the VMRay Analyzer Dashboard

One useful feature is a built-in progress bar that informs analysts just how far along their submission is. Depending on the analysis package, this saves analysts from refreshing until they have substantial results.

VMRay Analyzer's dashboard is also built to deliver knowledge in a way that suits the tool itself. VMRay Analyzer brings the answers to the relevant questions ("Is my sample done?" "Is my sample bad?") to the forefront. Lastly, as also provided in Figure 2, the analyst receives a final judgment as to whether the sample was determined to be benign, malicious or blacklisted.

Malware Analysis

No matter how easy a tool is to use, IR teams also need technical analysis that can help them make actionable decisions to help defend their organization. Remember, many organizations utilize tools to supplement team capabilities. If the tool is, at best, as good as the analyst, then it does not serve its purpose.

During our analysis, VMRay Analyzer proved itself an extremely effective malware-analysis tool.

Agentless Analysis

One standout attribute that increases VMRay Analyzer's effectiveness is the concept of agentless analysis. Let's break down how this works.

Some malware analysis platforms operate by spawning a virtual machine (VM) with special software installed. The special software, part of the analysis engine, or "sandbox," is responsible for executing the malicious code and monitoring changes to the system. These changes, such as registry key modifications or network connections, are captured and reported back to the malware analysis platform. Unfortunately, this is a static process that does not change between samples. To avoid analysis, malware authors have

found ways to detect the analysis agent and modify their system interactivity (thereby giving false data to the analysts). Some malware authors will even check for the analysis agent first and prevent any additional execution if the process is found.

VMRay caught on to these anti-forensic tricks and created a platform that removes the detectable analysis agent—thus, *agentless analysis*. VMRay uses a hypervisor to spawn analysis virtual machines, executing code within those VMs, and monitoring changes made via the hypervisor. With this capability, VMRay is able to execute and analyze malware more effectively than agent-based platforms. This advantage increases the volume of malware that an incident response team can analyze.

VMRay has advanced malware analysis through agentless analysis, which prevents malware from knowing it's being examined in a controlled environment.

VM Configurations

Another consideration when analyzing malware is the context of the system on which it was intended. Very few organizations have only one build within their environment. Consider retail environments, for example, which might utilize:

- Embedded Windows in the front-of-house terminals
- Standard Windows workstations for staff utilization
- A Windows Server in the back office to process transactions and facilitate store functions

Medical environments, universities and other organizations with multiple simultaneous functions also have a wide range of operating systems and configurations. The myriad of malware recovered from these environments can often lead to malware analysis issues that rely on one or two base operating systems. One of the key strengths of VMRay Analyzer, on the other hand, is being able to quickly test malicious files simultaneously in multiple operating systems. During our testing, we were presented with options including Windows 7, 32- and 64-bit, and Windows 10, 64-bit. See Figure 3.

Additionally, as shown in Figure 3, each analysis will have an option to choose a "Network Config" for **each** VM in which the analyst detonates the malware. This allows analysts to choose to run in an isolated mode to protect network callouts from tipping off attackers.

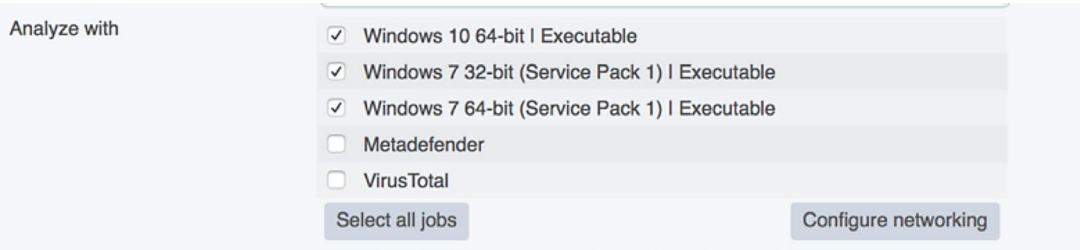

Figure 3. VMRay Analyzer VM Selection Menu

Utilizing a hypervisor to detect malware behavior gives VMRay Analyzer the ability to catalog and maintain multiple types of operating systems. Other platforms or manual setups may require that an analyst maintain multiple copies of VMs and multiple copies of monitoring/analysis tools.

As we tested the multiple VM management and utilization, one feature we wanted was the ability to produce and upload our own customized VMs. Many organizations have specific setups—such as custom, in-house software or specific versions of third-party applications—that are tough to replicate inside of a standard VM. Furthermore,

larger organizations will maintain standard or "gold" images that serve as baselines for deployed asset classes (such as laptops, desktops, etc.). Being able to convert these gold images into malware analysis engines allows the organization to *truly* test malware against its own environment.

VMRay has considered this possibility and created VMRay Auto Install Tool,[1] which automates the building of custom VMs for analysis. While that particular tool was out of scope for our testing purposes, we would highly encourage organizations to check it out.

The Reputation Engine

In addition to rethinking the malware sandboxing process, VMRay has built and included its massive Reputation Engine, VMRay's collection of known malicious and benign malware hashes that can be queried for uploaded samples. Different from a threat intel source, the Reputation Engine provides to IR teams a yes/no decision on maliciousness *within milliseconds*. To achieve this rapid decision, VMRay Analyzer embeds the reputation service from Reversing Labs. A subset of Reversing Labs data is cached locally to make reputation scoring even faster. The ability to determine whether a file is malicious this fast means that IR teams can make actionable decisions even faster, and analyze significantly larger volumes of malware.

VMRay's Reputation Engine allows for file classification within seconds, not minutes, allowing your team to get back to keeping the business safe.

VTI

The VMRay Threat Identifier, or VTI, engine is yet another powerful feature that speaks to VMRay's effectiveness. When samples are executed in VMs, the behavior exhibited by the malware is compared against VTI rules to determine a severity score, generally used to determine how malicious a file may be. The VTI engine has been a core piece of VMRay Analyzer since inception and remains one of its top features.

We especially liked VTI's rule customizability. During identification of malware, many tools or rulesets will focus on specific API calls that malware may use to achieve a task (such as download a file or enumerate a process). The problem is that there are multiple APIs that can achieve the same purpose—so how does a malware analyst prepare for them all? VMRay has devised an answer in the form of normalizing API calls to parent categories, such as "file download" or "process create." Instead of focusing on all the API calls, teams can focus on the behavior. This allows for faster building and deployment of rules.

Extending the Analysis with YARA

The last feature we will highlight is the inclusion of YARA rules. YARA is an open-source tool that allows for malware identification based on common signatures, such as strings or binary data included with an executable. YARA rules are files that contain

[1] VMRay blog, "Automating Custom VM Setups," April 7, 2016, www.vmray.com/blog/automating-custom-vm-setups

patterns respective to a malicious binary or particular strain of malware. YARA has been embraced by the security community, and there are currently thousands of YARA rules available for free. These rules provide rapid detection and classification of a significant portion of known advanced malware families.

The inclusion of YARA rules within VMRay Analyzer only enhances incident response capabilities. Incident response teams can build indicators that can be used to find malware samples based on similar heuristics. YARA also provides a platform for security teams to share and preserve indicators of compromise for posterity.

Increasing Efficiency with Integrations

VMRay Analyzer provides additional features to increase the potential effectiveness of your incident response team.

Imagine the following scenario: An incident response team member receives an alert that a suspicious executable was discovered on an HR system. There are two common types of incident response teams: siloed and integrated. Table 1 compares the response approach of each type.

If there's one thing that successful, efficient IR teams are doing more often than unsuccessful teams, it's the integration of multiple tools and platforms.

Note that the integrated team can often utilize integration and automation to respond to threats faster. Data can be provided within seconds, and threats neutralized within minutes.

VMRay Analyzer offers integration capabilities via two primary methods: API and out-of-the-box integrations.

Table 1. Siloed vs. Integrated Incident Response

Siloed Incident Response	Integrated Incident Response
• Analyst receives alert	• Analyst receives alert
• Consults host-based tools via one GUI	• Kicks off a process that automatically:
• Manually retrieves malicious file	- Captures suspicious executable from host-based platform
• Moves file across network to analysis system	- Forwards executable to VMRay and executes the malware in an environment that mimics the infected system
• Uploads file to malware analysis tool, or hands file off to malware specialist	- Delivers actionable results to analyst's inbox
• Waits until malware analysis is complete	• **Neutralizes threat within five minutes**
• **Neutralizes threat within an hour**	

API

VMRay Analyzer ships with a user-friendly RESTful API that allows for access to the tool's *full* functionality. This is a huge benefit for VMRay users, because it allows IR teams to build out and automate both submission of files *and* retrieval of analysis results. Some tools, for example, do not allow for data submission via the API, limiting the analysts to manual submission but automated results. VMRay's API also provides administrative functions, including capabilities such as adjusting configuration options, rescanning uploaded malware, and creating new analysis configurations. This will appeal to IR teams with programming or scripting capabilities, or a desire to customize their teams' interaction with the tool.

Integrations

IR teams without programming capabilities, and/or those that embrace pre-built cross-platform communication channels, will enjoy the out-of-the-box third-party integrations. VMRay currently has support for integration with the following platforms:

- OPSWAT
- Carbon Black
- Splunk
- ThreatConnect
- Ayehu
- VirusTotal
- MISP
- Phantom
- Demisto
- Swimlane
- LogicHub

Additionally, VMRay provides community resources to integrate VMRay with IR platforms such as TheHive, which allows incident response teams to centralize analysis and investigation updates. Integration with additional platforms allows organizations that already have solutions in place to utilize VMRay Analyzer as an effective malware-analysis tool. This has two benefits for integrated organizations:

- Endpoint detection and response tools are utilized for that function.
- Malware analysis and data collection is performed in VMRay, allowing the analysts to quarantine the host until a final decision can be made.

VMRay Analyzer in Action

The Malware

Despite all of the features and well-designed dashboard that a product may *claim* to have, it's all moot if the actual functionality of the product falls through. We put VMRay Analyzer through its paces using a handful of different malware types. The various malware we chose to sample were drawn from a pool of what many organizations are facing in today's environment:

- A malicious Excel workbook
- A malicious Word document
- A Macromedia Flash file that downloads the RIG Exploit Kit
- A Java Archive (JAR) masquerading as a PDF
- A Monero coin miner

Our questions remained the same for each sample:

- Does Analyzer *effectively* determine the file as malicious?
- *Why* does Analyzer determine the file as malicious?
- *How* does the VMRay VTI score compare to external lookups?
- Are there *benefits* to performing analysis in multiple virtual machines?

Lastly, we asked ourselves, "Does the tool *cater to both junior and senior analysts*?" The intent of this question was to explore whether Analyzer provides enough data that a junior analyst could make an informed decision, while a senior analyst is able to focus

on the options the tool presents for diving deeper. To explain the features and walk through the various details of the tool, we are going to focus on our results from the malicious Excel workbook.

Microsoft Office files, such as Excel workbooks, Word documents and PowerPoint presentations, are a seemingly endless source of threats. Figure 4 shows the initial results for our malicious workbook.

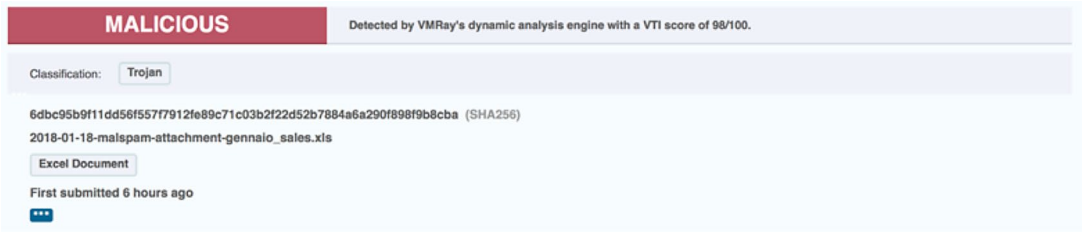

Figure 4. Malware Sample Data from VMRay Analyzer

Immediately, the analyst is drawn to the left side of the dashboard, which shows that this file has a blacklisted reputation score, as well as an extremely high (98/100) VTI score. Ignoring the Reputation Score for the moment (depending on the pace of an investigation, some teams could quickly pivot off of that score alone), let's examine how the file fared within our various VMs. Figure 5 provides a screenshot of the VTI results from each VM we tested the file in.

Note that our malware sample scored fairly high in each VM. For this sample, we utilized a sub-feature of VMRay's VM management, which allowed us to test the malware against one operating system, but *multiple versions of Microsoft Office*. This neat feature allowed us to determine whether it was a particular version of Office that was vulnerable—a very useful data point for organizations that are pegged to one version for a period of time.

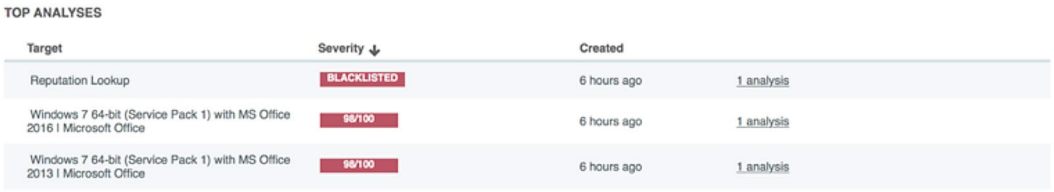

Figure 5. Malware Analysis Data from VMRay Analyzer

Let's examine the output for the VM with Office 2016. Clicking into any analysis result will launch you into the VMRay Analzyer Report, which again provides an easy-to-use interface bringing pertinent details to the forefront. Figure 6 provides a screenshot of the first section of the Analyzer Report.

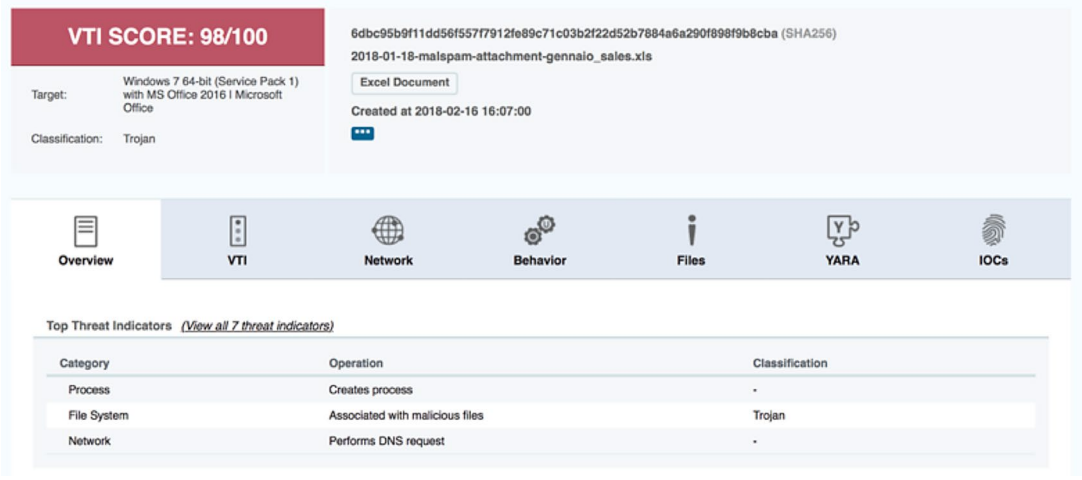

Figure 6. First Section of a VMRay Analyzer Report for a Malware Sample

The *Analysis Information* tab provides details about the sample run, such as filename, threat indicators and quick links to subset data points, such as VTI, Network and Behavior. Within the top pane there is an expandable "Download" button. This provides a one-stop source for analysts to download data about the sample run, such as a logfile, a PCAP of network connectivity, STIX/CybOX XML, and/or JSON data. This allows analysts, with one click, to integrate analysis results into other tools or detection

mechanisms. Examining the VTI tab, as seen in Figure 7, we can see what caused such a high VTI score.

Yet again, the scoring results are brought to the forefront so the analyst can quickly see that this malicious workbook created at least one suspicious process and contained a macro to spawn additional processes, among other attributes. The analyst can also pull out additional indicators from this section, such as the network address the malware reached.

Figure 7. VTI Scoring Data from a Malicious File in VMRay Analyzer

Returning to the main page for this particular analysis run, we can also determine subsequent children processes spawned by the malware. The first is within the "Monitored Processes" section, shown in Figure 8 of the main page.

Note that key process details are available on the front page. Furthermore, VMRay Analyzer will provide details as to *how* two processes are related; parent-child is the easiest, but the tool will also determine techniques such as code injection.

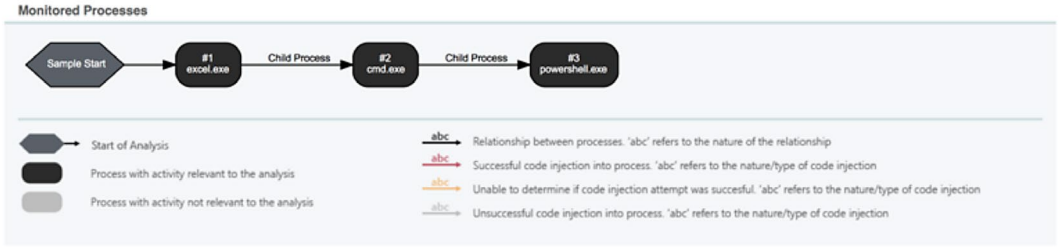

Figure 8. "Monitored Processes" from the Main Page of VMRay Analyzer

VMRay Analyzer presents an easy-to-follow analysis chain, in which we can see that the malware (first opened by **`excel.exe`** spawned **`cmd.exe`**, which in turn spawned **`powershell.exe`**. Analyzer allows us to drill down into each process, identifying the command-line processes, filename, working directory and other key attributes. Again, we are two clicks away from the main dashboard, and information is presented succinctly to the analyst.

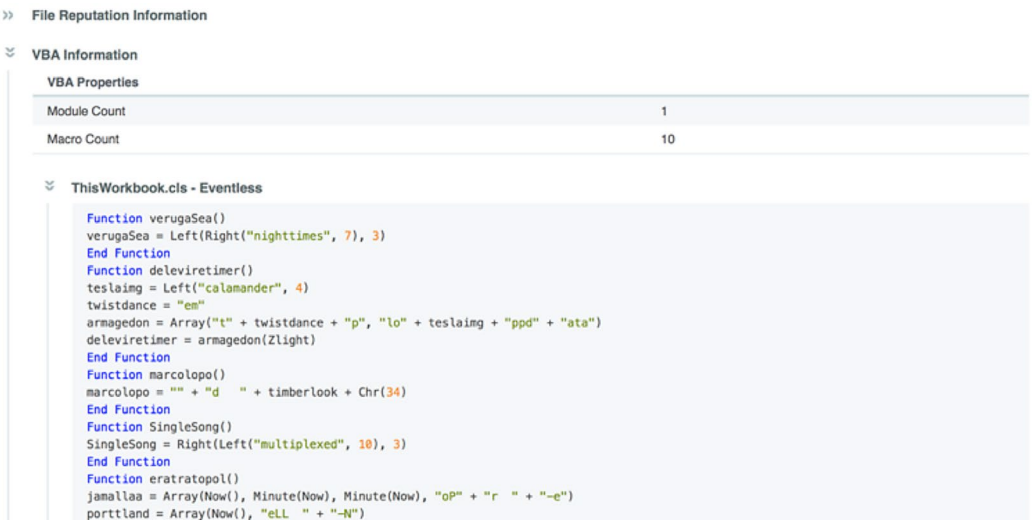

Figure 9. Files Data from a Malware Submission Within VMRay Analyzer

Lastly, one of our favorite features of testing Microsoft Office files within VMRay Analyzer was its ability to get us to the malicious code faster than other tools. Within the "Files" section, shown in Figure 9, analysts are presented with the option of actually diving into the VBA contained within the file.

Conclusion

The goal of any tool utilized by incident responders during times of crisis is to make the analysis of data and response to data breaches more efficient. Between easy-to-use interfaces, extensibility with a rich API and other platforms, and speedy analysis times, VMRay Analyzer provides a platform that helps IR teams do their job faster. Data is provided in a manner that allows those teams to operate with a higher level of confidence when protecting their organization.

While our testing was limited to a handful of samples of malware, we have confidence that VMRay Analyzer could easily scale into the hundreds or thousands of samples per day if need be. Additionally, our testing did not extensively utilize the API, but our brief testing, as well as exposure to third-party plugins, further qualifies it as a capable API. More importantly, the fact that VMRay Analyzer provides full tool functionality via the API means that teams with integration and automation in mind will find themselves able to utilize it fully without opening a browser. The concept of responding to breaches within *seconds or minutes* may seem impossible to some organizations, but with the right tools in place, IR teams at least have a fighting chance.

About the Author

Matt Bromiley is a SANS Digital Forensics and Incident Response instructor and a GIAC Advisory Board member. He is also a consulting director at a major incident response and forensic analysis company, bringing together experience in digital forensics, incident response/triage and log analytics. His skills include disk, database, memory and network forensics, as well as network security monitoring. Matt has worked with clients of all types and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor:

Last Updated: March 17th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SEC487: Open-Source Intel Beta One	McLean, VAUS	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Munich March 2018	Munich, DE	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Pen Test Austin 2018	Austin, TXUS	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, AU	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Boston Spring 2018	Boston, MAUS	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS 2018	Orlando, FLUS	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Abu Dhabi 2018	Abu Dhabi, AE	Apr 07, 2018 - Apr 12, 2018	Live Event
Pre-RSA® Conference Training	San Francisco, CAUS	Apr 11, 2018 - Apr 16, 2018	Live Event
SANS London April 2018	London, GB	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Zurich 2018	Zurich, CH	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MDUS	Apr 21, 2018 - Apr 28, 2018	Live Event
Blue Team Summit & Training 2018	Louisville, KYUS	Apr 23, 2018 - Apr 30, 2018	Live Event
SANS Seattle Spring 2018	Seattle, WAUS	Apr 23, 2018 - Apr 28, 2018	Live Event
SANS Doha 2018	Doha, QA	Apr 28, 2018 - May 03, 2018	Live Event
SANS Riyadh April 2018	Riyadh, SA	Apr 28, 2018 - May 03, 2018	Live Event
SANS SEC460: Enterprise Threat Beta Two	Crystal City, VAUS	Apr 30, 2018 - May 05, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, ILUS	May 01, 2018 - May 08, 2018	Live Event
SANS SEC504 in Thai 2018	Bangkok, TH	May 07, 2018 - May 12, 2018	Live Event
SANS Security West 2018	San Diego, CAUS	May 11, 2018 - May 18, 2018	Live Event
SANS Melbourne 2018	Melbourne, AU	May 14, 2018 - May 26, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VAUS	May 20, 2018 - May 25, 2018	Live Event
SANS Amsterdam May 2018	Amsterdam, NL	May 28, 2018 - Jun 02, 2018	Live Event
SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
ICS Security Summit & Training 2018	OnlineFLUS	Mar 18, 2018 - Mar 26, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced