

How VMRay Supports **Incident Response** in 4 Steps



How VMRay Supports Incident Response

Every Step of the Way:

STEP 1:

Operate immediately



Page 3



STEP 2:

Assess quickly



Page 4



STEP 3:

Investigate thoroughly



Page 11



STEP 4:

Document completely



Page 16

STEP 1:

Operate Immediately

Expedited Responses with Out of the Box Virtual Target Environments and Installed Software

As soon as an alert arrives, the clock is ticking like a timebomb – no wonder we call it a detonation. Your job is to assess, contain, investigate, eradicate and then respond and recover. With your business and brand on the line, it is a war against the attacker and against the clock, but VMRay multi-stage analysis along with widespread target environment coverage give you the power to fight back with completely automated analyses and detonations within the hypervisor sandbox. With VMRay Cloud you can be operating within minutes. With VMRay On Premises you can be operating within days and you retain complete control at your site.

Integrate seamlessly with your existing security infrastructure

VMRay allows you to integrate seamlessly with different tools in your security ecosystem such as your incident response or SOAR system – providing you with information you can trust in order to respond fast.

Enrich your [EDR/XDR](#), SIEM, [SOAR](#) and TIP to Curate your Own [Threat Intelligence](#)

With VMRay, you can enrich your SIEM, EDR/XDR, SIEM, TIP, web gateway alerts and curate your own threat intelligence so incident responders have the information at your fingertips to investigate an incident fast and comprehensively.

4 Input Options for Files, URLs and Emails – Both Automated and Ad Hoc

Quickly assimilate VMRay into your existing security stack with 4 different ways of inputting samples:

1. Through the Console – our easy-to-use GUI for ad hoc submission of files, URLs and emails.
2. Through the IR Mailbox – a common email address available to all end-users which auto-submits to VMRay – thereby empowering your entire end-user community to be cybersecurity protection participants.
3. Through one of our Connectors: from [Carbon Black](#) to [Sentinel One](#) to [Splunk](#) – industry leading software is supported so you can augment your EDR, SOAR, SIEM, TIP and more with automated submissions to VMRay.
4. Through our REST API – which gives you programmatic access to everything you see in the Console, including administrative functionality.

STEP 2:

Assess Quickly

Accurate and Actionable Verdicts and VTIs Eliminate Countless Wasted Hours

VMRay provides you with summary Verdicts and this is often all you need to respond. It is our overall judgement of a file or a URL that displays at the top of the very first report that you see: the Sample Overview report. Below that, our proprietary VMRay Threat Identifiers (VTIs) provide more detail related to specific threat behavior but without overwhelming you. Tabs on the Sample Overview report then allow you to dive as deep as you need to go and expand your investigation as required.

The Sample Overview Report Consolidates Key Information in a Single Spot

Everything you need to know about a file or URL is consolidated on the Sample Overview report so that you immediately understand the situation at a glance, including not just the Sample Verdict but the VTIs as well as the individual Analysis Verdicts, so that the situation in the precise environments you selected for analysis are immediately clear. This information enables you to act promptly, and it is your starting point for investigating further.

MALICIOUS

Classifications

-

Threat Names

Application.DealAlpha.1.Gen

SAMPLE OVERVIEW

fd9d728f645157fbbcf9257cf51d0f6e75e4f8e2c9edd75e3a6115a7159bd4cc.pe.exe

fd9d728f645157fbbcf9257cf51d0f6e75e4f8e2c9edd75e3a6115a7159bd4cc (SHA256)

Windows Exe (x86-32)

First submitted 3 days ago

...

Summary | **IOCs** 21 | **Analyses** 7 | Jobs | **ATT&CK™** 15 | Details | Comments

Analysis	Target Environment	Created ↓	Submitted by	Verdict	Actions
Dynamic	Windows 7 (SP1, 64-bit) exe	3 days ago	malicious_set@vmray.com	MALICIOUS	...
Dynamic	Windows 10 (TH1, 64-bit) exe	3 days ago	malicious_set@vmray.com	SUSPICIOUS	...
Dynamic	Windows 10 (19H2, 64-bit Latest) exe	3 days ago	malicious_set@vmray.com	SUSPICIOUS	...
Dynamic	Windows 7 (SP1, 32-bit) exe	3 days ago	malicious_set@vmray.com	MALICIOUS	...
Dynamic	Windows 8.1 (64-bit) exe	3 days ago	malicious_set@vmray.com	MALICIOUS	...
Dynamic	Windows 10 (19H1, 64-bit Latest) exe	3 days ago	malicious_set@vmray.com	SUSPICIOUS	...
Static	Default static configuration	3 days ago	malicious_set@vmray.com	SUSPICIOUS	...

Verdicts – What You Need to Know Now

Three high-level verdicts are often all you need to know now: is it Clean, Suspicious or Malicious? Use them to eliminate false positives and validate true positives. Classifications and Threat Names help you start with damage assessment and response formulation.

MALICIOUS

Classifications

Ransomware

Threat Names

Sodinokibi | Mal/Generic-S |
Trojan.GenericKD.46595146 |
Gen:Variant.Ransom.Sodinokibi.61

SUSPICIOUS

Classifications

–

Threat Names

Application.DealAlpha.1.Gen

CLEAN



Classifications

–

Threat Names

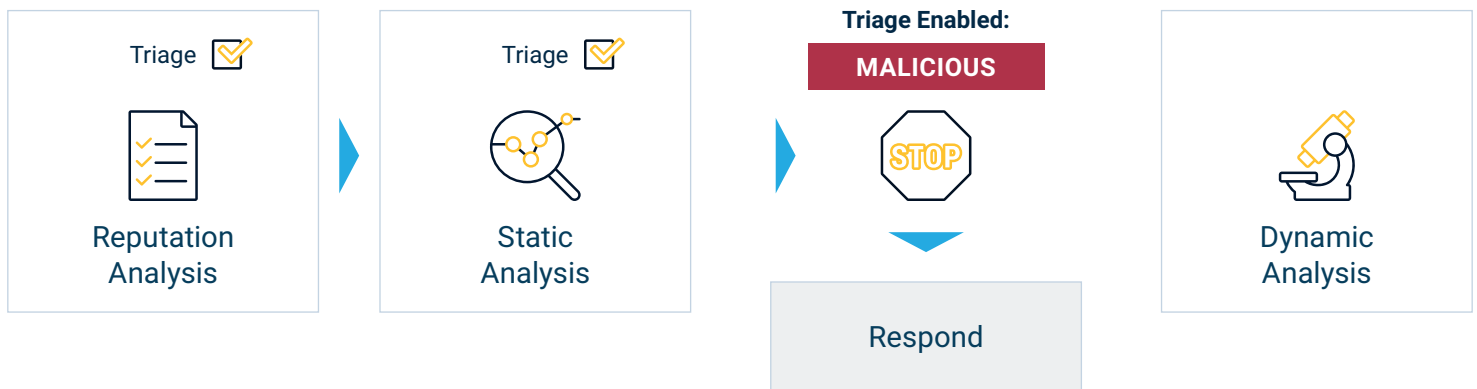
–



Triage Helps you Minimize Response Times

When it comes to a response, ASAP isn't fast enough. It needs to be done yesterday. So we've built in as many time saving tools as possible for you – one of which is pre-filtering of samples during Reputation Analysis and Static Analysis, so that Dynamic Analysis and Web Analysis need not be performed if it is not needed. Instead, you can initiate triage and start formulating your response immediately.

A commonly used application of this is to triage Malicious files, as illustrated below, where Reputation Analysis and Static Analysis both have Triage Enabled for Malicious files, which means that if either one of these analyses assigns a Malicious verdict to the file, the analysis is stopped immediately before Dynamic Analysis starts. This not only reduces your quota usage, but more importantly, it enables you to respond to the Malicious file immediately. Of course, you can manually perform Dynamic Analysis on the file if you want to investigate further, but triage ensures that you can take action right away to mitigate the threat.



VTI Scores – When You Need to Know More

When a bit more detail is needed, our proprietary VMRay Threat Identifiers (VTIs) provide a concise and visual summary of the findings, all rated on a scale of 1 to 5. So you get more information beyond the verdict, but doled out in convenient bite-sized pieces.

VMRay Threat Identifiers (21 rules, 253 matches)

	Score	Category	Operation	Count	Classification
▶	5/5	User Data Modification	Modifies content of user files	1	Ransomware
▶	5/5	User Data Modification	Deletes user files	1	Wiper
▶	5/5	YARA	Malicious content matched by YARA rules	100	Ransomware
▶	5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
▶	5/5	User Data Modification	Modifies Windows automatic backups	1	-
▶	4/5	Antivirus	Malicious content was detected by heuristic scan	8	-
▶	4/5	Privilege Escalation	Creates elevated child process	1	-
▶	2/5	Anti Analysis	Tries to detect virtual machine	1	-

Individual VTI scores on the Sample Overview Report all have more details available with a click, and the context-action-menus enable deep dives with a second click, as in this example which hyperlinks you to the Files tab which has complete details about this problematic file which looks like a ransom note:

3/5 User Data Modification Possibly drops ransom note files 1 Ransomware

- (Process #8) mspeng.exe possibly drops ransom note files (creates 65 instances of the file "gc77ux2-readme.txt" in different locations). ...

Go to File Details

Automated Web Analysis Identifies Phishing Attempts by URLs

Not only does VMRay detonate a multitude of file types, but URLs as well, so that phishing attempts are identified and can be prevented. The Automated user simulation (known as Auto UI), which is built-in to Web Analysis, ensures a comprehensive detonation, and results in detailed reports analyzing all aspects of a phishing attempt.

Automated user simulation can be augmented with Live Interaction which allows you to manually interact with the malicious URL (e.g., as it tries to harvest credentials) to further flush out malicious behavior that automation might not catch.

MALICIOUS
🔄

Classifications
Phishing

Threat Names
-

SAMPLE OVERVIEW

<https://cracker.new.razorproductions.com/.well-known/pki-validation/chase/>

URL

First submitted 1 day ago

...

Summary
IOCs 8
Analyses 1
Jobs 4
ATT&CK™
Details
Comments

TOP ANALYSES

Analysis	Target Environment	Created		Verdict	
Web	VMRay Web Analyzer Automated	24 hours ago	1 analysis	4 jobs	MALICIOUS

VMRAY THREAT IDENTIFIERS

Score	Category	Operation	Classification
5/5	Heuristics	Page is determined to be phishing attempt	Phishing
2/5	Heuristics	Page secured via a Domain Validated SSL certificate	-
2/5	Masquerade	Page uses exact favicon of an online financial service	-
1/5	Heuristics	Page presents itself as a logon page	-

All is Revealed During Detonation with Live Interaction

To flush out the full behavior of malware, the sandbox's Auto UI executes user interactions for you during Dynamic Analysis of files and Web Analysis of URLs. But you can augment this with your own human interaction - or Live Interaction as we call it.

This can be turned on for either Web Analysis or Dynamic Analysis - at the time of submission, as in this example where Windows 10 running on Internet Explorer (ie) is selected for Live Interaction during Dynamic Analysis of a URL.

Live Interaction	<input checked="" type="checkbox"/>	Interact with the sample during Dynamic or Web Analysis
Web Analysis ?	<input type="checkbox"/>	win7_64_url Automated
	<input type="checkbox"/>	win7_64_url Interactive
Dynamic Analysis ?	<input checked="" type="checkbox"/>	Windows 10 (RS2, 64-bit) ie
	<input type="checkbox"/>	Windows 7 (SP1, 32-bit) ie
	<input type="checkbox"/>	Windows 7 (SP1, 64-bit) ie

Easy to use MITRE ATT&CK Matrix with Mapped VTIs

We make it easy to use the industry standard MITRE ATT&CK matrix by highlighting only cells that are relevant and mapping our color-coded VTIs to them.

Summary IOCs 45 Analyses 21 Jobs ATT&CK™ 12 Details Comments

MITRE ATT&CK™ Matrix - Windows

ACTIVE ALL

Version: 2019-04-25 20:53:07.719000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	Scheduled Task	Scheduled Task	Scheduled Task	Hidden Window	Credentials in Registry	System Information Discovery		Automated Collection			
				Software Packing	Credentials in Files	Query Registry		Data from Local System			
					Credential Dumping	Browser Bookmark Discovery					
						File and Directory Discovery					

Clicking on any cell in the matrix provides you with a correlation back to the corresponding VTIs, and provides detailed information about the MITRE technique itself, as in the example above of Automated Collection, which corresponds to our own Data Collection VTI category:

Automated Collection



Corresponding VMRay Threat Identifiers (5)

Score	Category	Operation
5/5	Data Collection	Tries to read cached credentials of various applications
2/5	Data Collection	Reads sensitive ftp data
2/5	Data Collection	Reads sensitive mail data
2/5	Data Collection	Reads sensitive application data
2/5	Data Collection	Reads sensitive browser data

Technique Information

ID:	T1119
Tactics:	Collection
Platform:	Linux, macOS, Windows

Once established within a system or network, an adversary may use automated techniques for collecting internal data. Methods for performing this technique could include use of [Scripting](#) to search for and copy information fitting set criteria such as file type, location, or name at specific time intervals. This functionality could also be built into remote access tools.

This technique may incorporate use of other techniques such as [File and Directory Discovery](#) and [Remote File Copy](#) to identify and move files.

You can dive even deeper into the VTIs from here, and see specific file information:

Host Behavior

Operation	Filename	Additional Information	Success	Count	Logfile
Create	C:\Windows\system32\Serverx.exe	file_attributes = FILE_ATTRIBUTE_DIRECTORY	✓	1	FN

Click on the FN button (on the far right) to dive to the very deepest level and see the exact call for this file, highlighted in the Function Logfile:

Function Logfile



```
898. [0071.916] WinExec (lpCmdLine="\C:\Users\Sp5NrGJn0jS HALPmcxz\Desktop\afc420e21457514af091006cb3bbbae24241b8dda00666052da2badff85445b0.pe.exe" ", uCmdShow=
899. [0101.253] Sleep (dwMilliseconds=0x2710)
900. [0112.647] GetSystemTime (in: lpSystemTime=0x18ed0c | out: lpSystemTime=0x18ed0c*(wYear=0x7e5, wMonth=0x8, wDayOfWeek=0x1, wDay=0x9, wHour=0x13, wMinute=0x30, wS
901. [0112.647] RegOpenKeyA (in: hKey=0x80000002, lpSubKey="SYSTEM\\CurrentControlSet\\Services\\LanmanServer\\Parameters", phkResult=0x18fe38 | out: phkResult=0x18fe
902. [0112.649] RegSetValueExA (in: hKey=0xa8, lpValueName="AutoShareServer", Reserved=0x0, dwType=0x4, lpData=0x4228df*-0x0, cbData=0x4 | out: lpData=0x4228df*-0x0)
903. [0112.652] RegOpenKeyA (in: hKey=0x80000002, lpSubKey="SYSTEM\\CurrentControlSet\\Services\\LanmanServer\\Parameters", phkResult=0x18fe38 | out: phkResult=0x18fe
904. [0112.652] RegSetValueExA (in: hKey=0xac, lpValueName="AutoShareWks", Reserved=0x0, dwType=0x4, lpData=0x42295a*-0x0, cbData=0x4 | out: lpData=0x42295a*-0x0) ret
905. [0112.652] GetSystemDirectoryA (in: lpBuffer=0x18fd3c, uSize=0x100 | out: lpBuffer="C:\\Windows\\system32") returned 0x13
906. [0112.653] _lcreat (lpPathName="C:\\Windows\\system32\\Serverx.exe" (normalized: "c:\\windows\\syswow64\\serverx.exe"), lAttribute=16) returned 0xb4
907. [0112.708] RtlUnicodeStringToAnsiString (in: DestinationString=0x18fbe0, SourceString="\\??\\C:\\Windows\\system32\\Serverx.exe", AllocateDestinationString=0 | c
908. [0112.745] GetTickCount () returned 0xc3ef45
909. [0112.772] CreateFileA (lpFileName="C:\\WINDOWS\\SYSTEM32\\SERVERX.EXE" (normalized: "c:\\windows\\syswow64\\serverx.exe"), dwDesiredAccess=0x80000000, dwShareM
910. [0112.774] _hwrite (in: hFile=0xb4, lpBuffer=0x18fd34*, lBytes=1 | out: lpBuffer=0x18fd34*) returned 1
911. [0112.775] _hwrite (in: hFile=0xb4, lpBuffer=0x18fd34*, lBytes=1 | out: lpBuffer=0x18fd34*) returned 1
```

Function Name	Line Number
_lcreat	906

STEP 3:

Investigate Thoroughly

The Deepest Possible Dives with Detailed Analysis Reports and Sandbox Detonations

Beyond the Sample Overview Report, you have detailed reports for: Reputation Analysis, Static Analysis, Dynamic Analysis and Web Analysis. The last two report on detonation within the Sandbox, thereby providing comprehensive visibility into the entire range of malware behavior. This is particularly useful for identifying and classifying those especially dangerous malware which is advanced, targeted and complex, that is, those threats that have never been seen before.

We transform the unknown into known by detonating in a wide range of different target environments and providing you with detailed reports that include screenshots and process diagrams so you can see the exact behavior of the malware. All detonations use the Sandbox which doesn't change a single bit or byte of information in the VM and so our sandbox is almost impossible to evade – even for the most savvy of attackers.



4 Detailed Reports Including Two Displaying Detonations

While the Sample Overview summarizes the Verdict, the VTIs and other key information – when you need to investigate further – there are up to four additional report types that provide more detail: Reputation, Static, Dynamic and Web Analysis Reports. Samples are detonated during Web Analysis and Dynamic Analysis so you can see a complete series of screenshots of the explosion in these reports, and for files, you also get a complete process flow diagram highlighting red flags.

You are barraged by alerts – some valid and some not. IR only begins when you verify that an alert is indeed an incident so we clarify which of them are red alerts so that you can respond only when the threat is real.


MALICIOUS

Sample Overview

VTI 5/5
VTI 4/5

MALICIOUS


Reputation Report



VTI 5/5
VTI 4/5

MALICIOUS


Static Analysis Report




VTI 5/5
VTI 4/5


MALICIOUS

Web Analysis Report




VTI 5/5
VTI 4/5







MALICIOUS


Dynamic Analysis Report



VTI 5/5
VTI 4/5







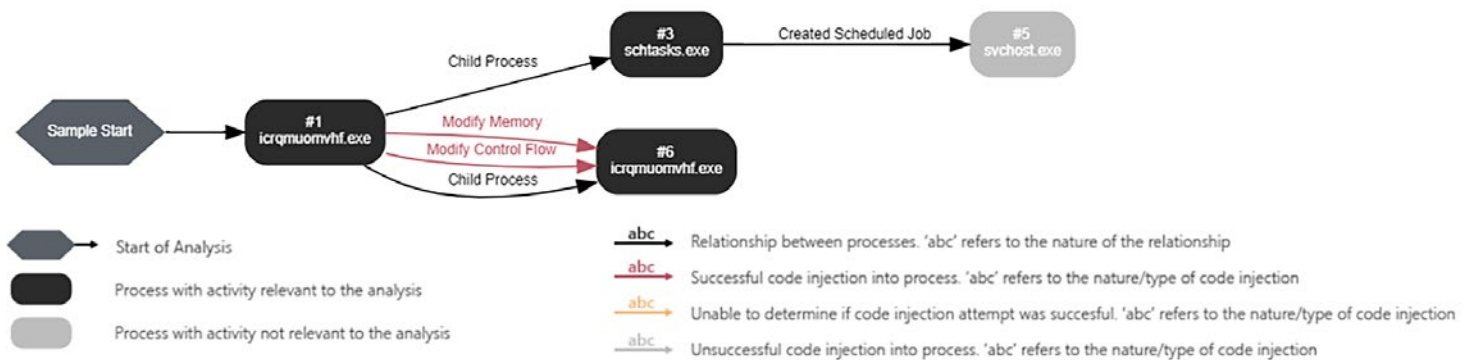
See the File Detonation for Yourself with Screenshots and Monitored Processes

After the Dynamic Analysis of a file has been performed, you can see the detonation for yourself on the Dynamic Analysis Report, with screenshots of the entire sequence, and you can look at the process flow too – where red flags immediately jump out because they are highlighted with red lines and red text:

Screenshots



Monitored Processes



Get the Gold: IOCs are Sifted and Sorted For You

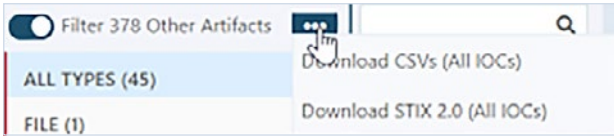
Gold-miners sift through stones and sediment for gold. Analysts sift through artifacts for IOCs. So we do the serious sifting for you by extracting those all-important IOCs from everyday artifacts, and each is assigned their own verdict, which in turn informs the overall verdict. IOCs are also conveniently sorted into categories to make your analysis even easier: files, IPs, mutexes, and processes, as in the example below, where there are 423 total artifacts, but only 45 IOCs worth looking at, so 378 artifacts are hidden from view.

Summary | **IOCs (45)** | Analyses (21) | Jobs | ATT&CK™ (12) | Details | Comments

Filter 378 Other Artifacts

Type	Value	Details Preview	Verdict	Actions
File	icrqmuomvhf.exe +23	Sample File, Binary	MALICIOUS	...
Process	icrqmuomvhf.exe	"C:\Users\jHik7hbkQ\Desktop...	MALICIOUS	...
Process	icrqmuomvhf.exe	"C:\Users\FD1HVY\Desktop...	MALICIOUS	...
Process	icrqmuomvhf.exe	"C:\Users\OE4rt08B\Desktop...	MALICIOUS	...
Process	icrqmuomvhf.exe	"C:\Users\UH34m5\Desktop...	MALICIOUS	...

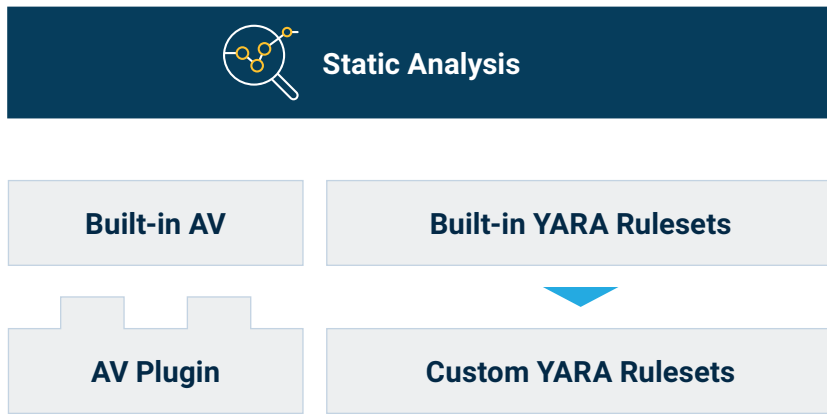
Export in CSV or STIX JSON for further analysis:



Comprehensive Analytical Coverage including the Basics: Built-in AV and YARA Rulesets

While VMRay is known for its best-of-breed hypervisor-based sandbox, we also cover the basics with built-in Antivirus (AV) checking of our own during Static Analysis, as well as built-in YARA matching using our own proprietary YARA Rules. During our built-in AV scan, we not only scan the file, but also all network data and memory dumps too.

So, while VMRay is ultra-sophisticated and geared towards identifying and analyzing advanced threats, we also make sure known threat patterns are identified too. On Premises customers can even augment our AV with your own, or with another third-party AV engine, using the AV Plugin.



The resulting VTIs related to YARA and AV display as VTIs. Often, there is no need to detonate if the threat is detected early in the analysis workflow, as in this example, where the sample can be immediately triaged based on the fact that YARA and AV have clearly identified this sample as a problem.

VMRay Threat Identifiers (21 rules, 253 matches)

	Score	Category	Operation	Count	Classification
▶	5/5	YARA	Malicious content matched by YARA rules	100	Ransomware
▶	4/5	Antivirus	Malicious content was detected by heuristic scan	8	-

YARA matches are based on our own proprietary tried-and-true YARA Rulesets which work out of the box, but which you can also easily customize or extend.

These YARA Rulesets have been meticulously researched and improved over many years so you can safely rely on them to identify all of those terrifying TLAs (Three-Letter Acronyms) that keep analysts up at night: from APTs to CVEs to PUAs to RATs, and many more.

YARA RULESETS

ID	Type	Owner	Name
#1	Built-in	VMRay	APTs
#2	Built-in	VMRay	CVEs
#3	Built-in	VMRay	Exploit-Kits
#4	Built-in	VMRay	Generic
#5	Built-in	VMRay	Hacktools
#6	Built-in	VMRay	Malicious-Documents
#7	Built-in	VMRay	Malware
#9	Built-in	VMRay	Payloads
#8	Built-in	VMRay	PUAs
#11	Built-in	VMRay	Ransomware
#10	Built-in	VMRay	RATs

STEP 4:

Document Completely

Fighting Back Against Targeted Attacks: Golden Images for On Premises Customers

Golden images are supported with our Auto Install Tool, which allows the automated creation and deployment of fully customized VM target environments that mimic your actual end-user environments. Targeted malware is particularly dangerous but we enable you to fight back with life-like target environments that replicate real-world systems: from geolocation settings like location, GUI language and keyboard settings to filling up file folders to make the VM look real to randomizing the usage of a desktop image. Golden images allow for real-world detonation within our VMs instead of on your actual company computers.

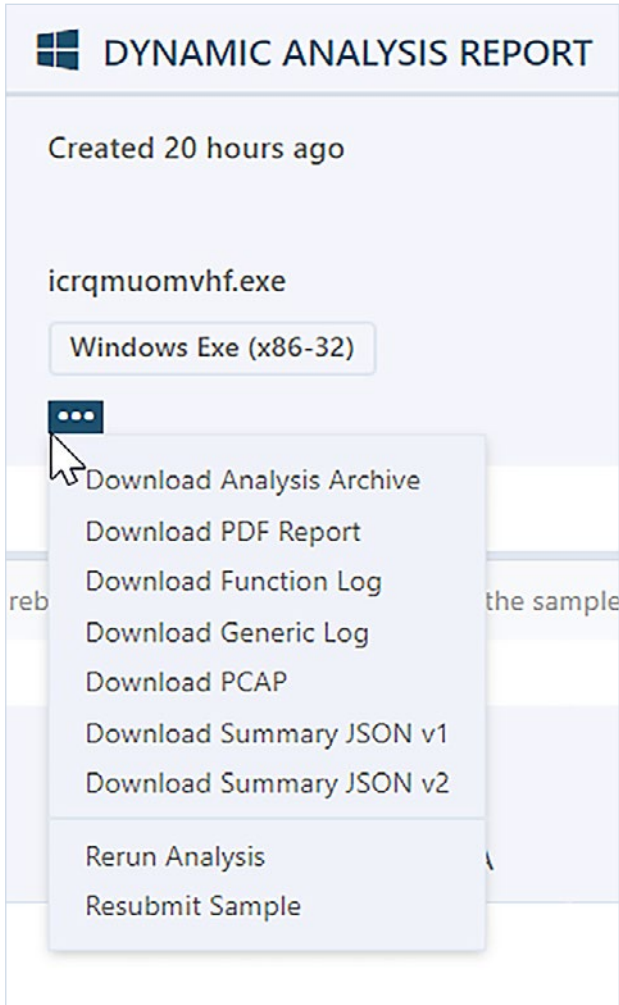
A to Z Coverage: Analysis Archive to PDF to STIX to ZIPs

Incidents often involve a crime and so, just like a crime, evidence needs to be collected and documented and VMRay helps you here too. For the initial stages, there are customizable and brandable PDF reports of the Sample Overview report and for all four detailed reports, right through to the final stages, where we have a comprehensive Analysis Archive which bundles every artifact into a single ZIP file for convenient archiving, including all dropped, downloaded and created files, all function calls, PCAPs and reports of all relevant network traffic, STIX reports, memory dumps, screenshots, and our own proprietary Summary.json, as well as everything in between. You want to close the case quickly but you have to check off due diligence and that involves documenting everything you find in your assessment and investigation. It's no fun for anyone but at least we streamline the path for you and automate report creation wherever possible.



A Wide Variety of Output Options Available on Every Report

From the very lowest level Analysis Archive, which has every imaginable artifact of the analysis, to the high-level PDF reports which are ideal for management, you can output as you please using the Action menus on each report, such as these on the Dynamic Analysis Report:



Brandable PDF Reports for Management

Incidents inevitably get escalated, increasingly to the very top these days, so we provide sleek reports that are easy for anyone to read, and the reports can be branded with your own title and logo. Just like our online reports, the PDF reports start with a noise-free summary that includes the Verdict and VTIs, but then later in the report, detailed information is available when your readers need to know more, even including screenshots of the detonation itself.



ABC Company CERT

Detailed Analysis Report

MALICIOUS

Classifications: **Spyware**

Threat Names: **Lokibot** **Trojan.GenericKDZ.76183** **Gen:Variant.Razy.762033**

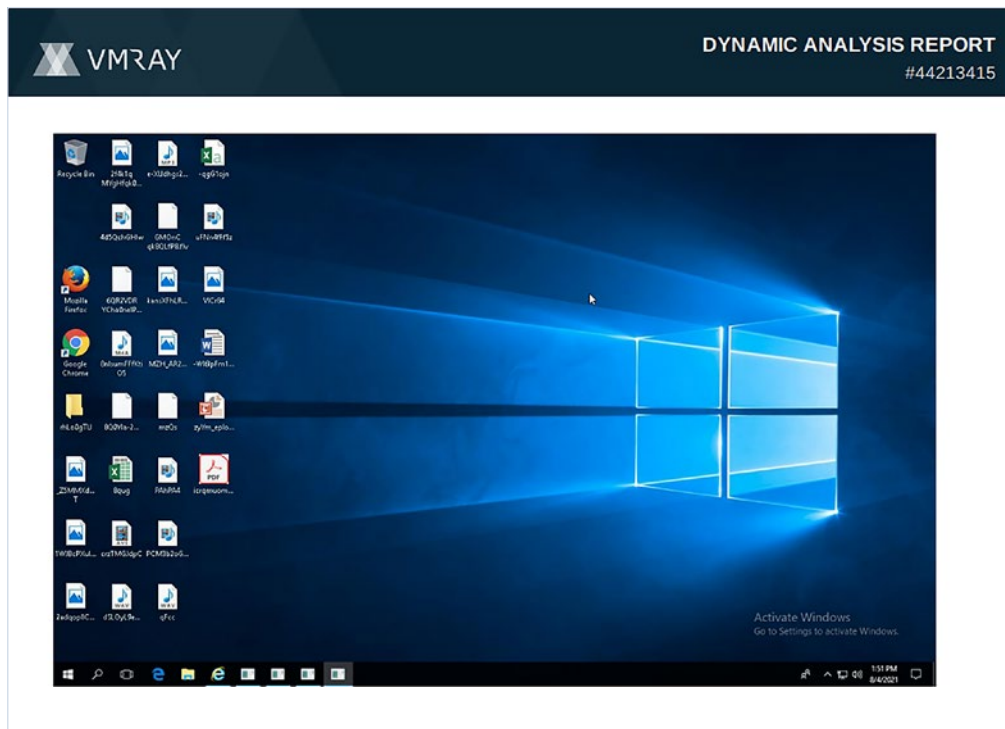
Verdict Reason: -

Sample Type	Windows Exe (x86-32)
File Name	icrqmuomvhl.exe
ID	#7243590
MD5	f1e712d502a4f228cdcfc6f5f994240d
SHA1	279e05f2c52f25cc2102fd5f7420e3a7e425d31d
SHA256	7ec6c06ce36ba89c2b9123531436f361380a435f6c1a6374820525aad6ea4d9f

OVERVIEW

VMRay Threat Identifiers (21 rules, 62 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	Spyware
<ul style="list-style-type: none"> • Rule "Lokibot" from ruleset "Malware" has matched on a memory dump for (process #6) icrqmuomvhf.exe. 				
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
<ul style="list-style-type: none"> • Tries to read sensitive data of: BlazeFTP, Bitvise SSH Client, LinasFTP, NCH Classic FTP, Opera Mail, Trojita, Pidgin, FTP Navigat... ..Chips, Total Commander, QWeb Internet Browser, Internet Explorer, Pocomail, KITTY, PuTTY, FAR Manager, SecureFX, Mozilla Firefox. 				
4/5	Antivirus	Malicious content was detected by heuristic scan	2	-
<ul style="list-style-type: none"> • Built-in AV detected the sample itself as "Trojan.GenericKDZ.76183". • Built-in AV detected a memory dump of (process #6) icrqmuomvhf.exe as "Gen:Variant.Razy.762033". 				
3/5	Discovery	Reads installed applications	1	Spyware
<ul style="list-style-type: none"> • Reads installed programs by enumerating the SOFTWARE registry key. 				



Deep Dives with Smart Memory Dumps

Malware usually is packed, encrypted, and obfuscated to evade signature detection. In order to execute though, it needs to unpack in memory so they can execute as intended and this creates an opportunity for VMRay to detect potentially malicious behavior during detonation in the hypervisor sandbox. So VMRay triggers a succession of memory dumps, creating snapshots of telltale information about a potential threat or attack. Incident responders love the level of detail provided in our smart memory dumps which capture a complete and accurate record of malware behavior, right down to the exact function calls and corresponding memory addresses.

Memory Dumps

Name	Start VA	End VA	Dump Reason	PE Rebuilds	Bitness	Entry Points	AV	YARA	Actions
microsoftofficeword_upd.v.88735.34.5.exe	0x400000	0x4b8fff	Relevant Image	X	32-Bit		X	X	...
microsoftofficeword_upd.v.88735.34.5.exe	0x400000	0x4b8fff	Process Termination	X	32-Bit		X	X	...
buffer	0x1d80000	0x1dacfff	First Execution	X	32-Bit	0x1d80000	X	X	...
buffer	0x1d80000	0x1dacfff	Content Changed	X	32-Bit	0x1d83124	X	X	...
buffer	0x1d80000	0x1dacfff	Content Changed	X	32-Bit	0x1d84994	X	X	...
buffer	0x1dc0000	0x1dc0fff	First Execution	X	32-Bit	0x1dc0000	X	X	...

Deepest Dives with Function Logs

Unlike traditional sandboxing, VMRay's intelligent monitoring technology always provides the highest semantic level possible, that is, it does not matter if the malware is using Java/COM methods, Win32 APIs, Native APIs, or direct system calls. VMRay monitors and reports all of them, including call parameters, return values, and memory content. Also unlike other sandboxes, VMRay monitors kernel code execution and MBR modifications, to also detect the most sophisticated kernel rootkits.

Function logs take you to this lowest level of detail and display all individual calls:

Function Logfile



```

25805. [0062.609] VirtualAlloc (lpAddress=0x0, dwSize=0x1000, flAllocationType=0x3000, flProtect=0x40) returned 0x2190000
25806. [0062.631] VirtualFree (lpAddress=0x2190000, dwSize=0x0, dwFreeType=0x8000) returned 1
25807. [0062.635] GetModuleFileNameW (in: hModule=0x0, lpFilename=0x17e900, nSize=0x104 | out: lpFilename="C:\\Windows\\Temp\\Microso
25808. [0062.638] CreateProcessW (in: lpApplicationName=0x0, lpCommandLine="C:\\Windows\\Temp\\MicrosoftOfficeWord_upd.v.88735.34.5.
25809. [0062.642] GetThreadContext (in: hThread=0x1dc, lpContext=0x17e580 | out: lpContext=0x17e580*(ContextFlags=0x1003f, Dr0=0x0,
25810. [0062.643] NtQueryInformationProcess (in: ProcessHandle=0x1e0, ProcessInformationClass=0x0, ProcessInformation=0x17e338, Proc
25811. [0062.644] ReadProcessMemory (in: hProcess=0x1e0, lpBaseAddress=0x7efde000, lpBuffer=0x17e378, nSize=0x1e8, lpNumberOfBytesRe
25812. [0062.644] VirtualProtectEx (in: hProcess=0x1e0, lpAddress=0x400000, dwSize=0x2c000, flNewProtect=0x4, lpflOldProtect=0x17e57
25813. [0062.644] WriteProcessMemory (in: hProcess=0x1e0, lpBaseAddress=0x400000, lpBuffer=0x729e0048*, nSize=0x2c000, lpNumberOfbyt
25814. [0062.659] VirtualProtectEx (in: hProcess=0x1e0, lpAddress=0x400000, dwSize=0x400, flNewProtect=0x2, lpflOldProtect=0x17e36c
25815. [0062.660] VirtualProtectEx (in: hProcess=0x1e0, lpAddress=0x401000, dwSize=0xac34, flNewProtect=0x20, lpflOldProtect=0x17e36
25816. [0062.660] VirtualProtectEx (in: hProcess=0x1e0, lpAddress=0x40c000, dwSize=0x2b2e, flNewProtect=0x2, lpflOldProtect=0x17e36c
25817. [0062.660] VirtualProtectEx (in: hProcess=0x1e0, lpAddress=0x40f000, dwSize=0xe690, flNewProtect=0x4, lpflOldProtect=0x17e36c
25818. [0062.660] VirtualProtectEx (in: hProcess=0x1e0, lpAddress=0x41e000, dwSize=0xc800, flNewProtect=0x4, lpflOldProtect=0x17e36c

```

Function Name

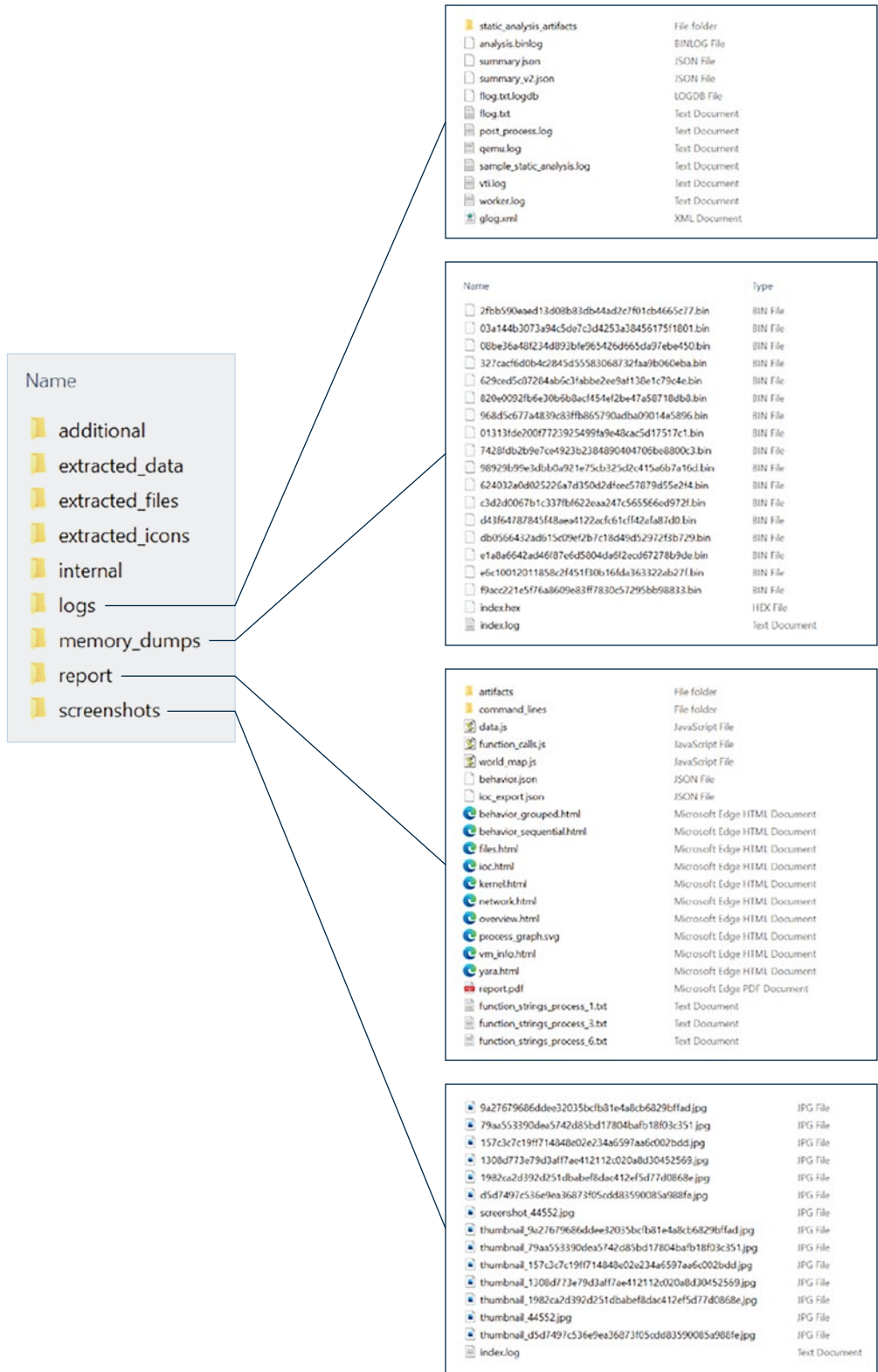
Line Number

WriteProcessMemory

25813

Case Closed – The Analysis Archive

When the case is closed, the files go into the archive, so the provided Analysis Archive is ideal for this because it has a comprehensive collection of all reports, logs, screenshots, memory dumps and much more – all within a single file for easy archiving and retrieval at a later date. Just some of the files are depicted below.



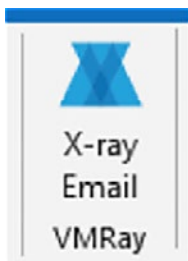
Automate, Extend, Customize and Much More

Ultimate Automation Flexibility and Complete Customizability

VMRay and its underlying Platform are designed to be an integral part of your security ecosystem so we provide a multitude of tools and methods for enhancing and extending and connecting VMRay to industry-leading tools and software. From a simple Outlook Plugin that lets end-users submit to VMRay's IR Mailbox, to Connectors that hook you up to industry-leading SIEM, SOAR, EDR, TIP and MDR software, everything you need to build a completely unique ecosystem and an unbeatable cyber defence system is available.

Outlook Plugin for IR Mailbox

In the fight against cyber attacks, every possible ally is needed, and this can include the hundreds, thousands, or even tens of thousands of end users – the large majority of whom are now working remotely. With the IR Mailbox, they have a convenient and centralized email address for submitting suspicious emails, which are in turn, submitted to VMRay. Take this one step further and use the Outlook Plugin to place a button in the toolbar of Outlook and give your end users one-click access to the IR Mailbox.

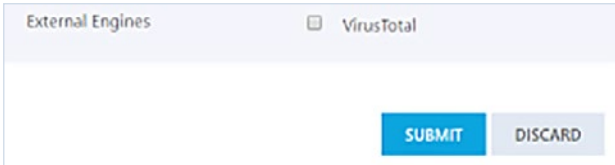


Optionally Augment Analyses with VirusTotal

Recognizing VirusTotal as an industry standard, you can optionally add pre-built VirusTotal configurations to your standard analyses:

macOS Mach-O		
ID	Signature	Analyzer
224	vmray:macos_10.13.1:def:macos_exe	Dynamic
101	virustotal	VirusTotal
Custom		
ID	Signature	Analyzer
3	vmray:win7_64_sp1:def:by_ext	Dynamic
13	virustotal	VirusTotal
Windows Help File		
ID	Signature	Analyzer
85	vmray:win10_64_rs2:def:chm	Dynamic
88	virustotal	VirusTotal

So that all a user has to do is select VirusTotal before submission:



Connect with Ease to Other Industry Leaders

VMRay is the perfect supplement to your existing security stack – from SIEM to SOAR to EDR/XDR and TIP too – we have Connectors to industry-leading security software that you can use to plug into VMRay. Most feature the ability to input the file and URL samples to VMRay, and to ingest the resulting output from VMRay back in.



SOAR



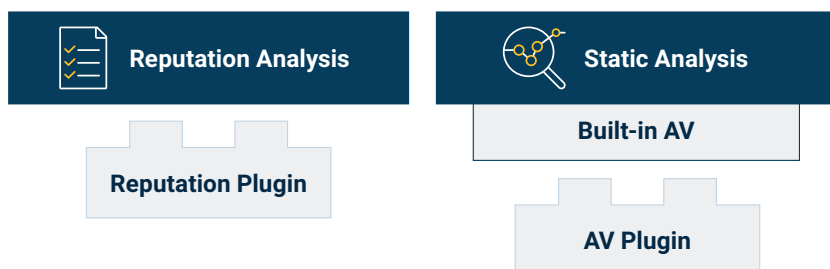
EDR / XDR



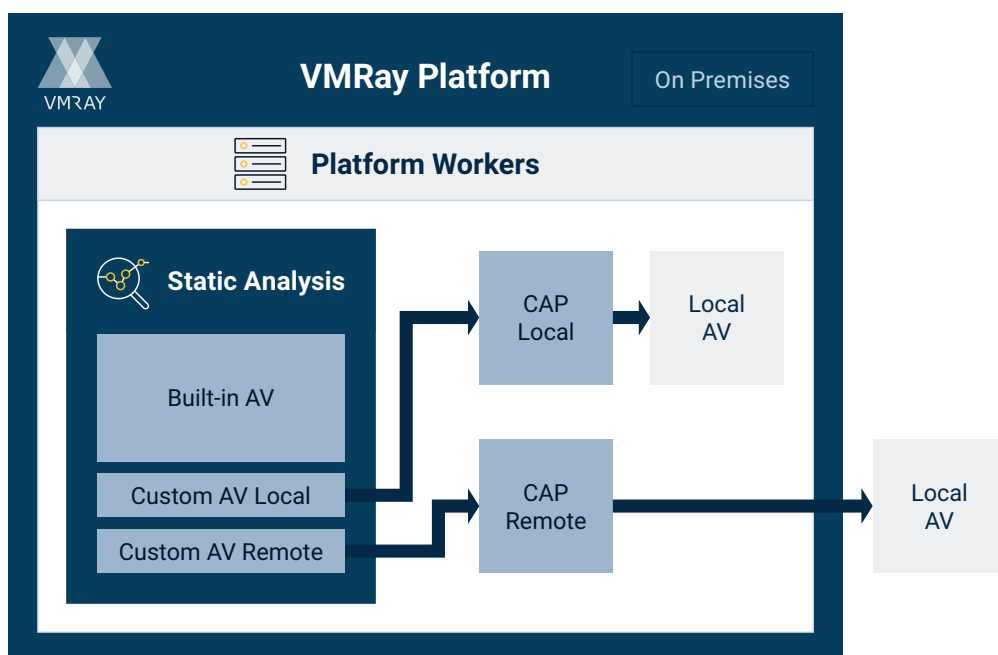
TIP / SIEM

Reputation Analysis and AV Plugins – Augment as Needed

Here is yet another feature that we created for our power users who are pushing VMRay to the limit: our Reputation Analysis and Built-in AV Antivirus check often suffice, but when needed you can augment both with easy-to-customize plugins. One breach can be catastrophic for your company, so the more lines of defense the better, and we give you the ability to implement them quickly.



For example, our Built-in AV is invoked automatically during Static Analysis, but you can augment this AV with either Local AV or a Remote AV can be 'plugged' in to add 1-2 more levels of Antivirus protection:



Extend your Techniques by Customizing our VTIs

The VTIs you see on the reports are powered by an underlying VTI engine. For our power users who want the ultimate in customization, these VTI rules can be extended and augmented. Out of the box, we provide over 20 VTI categories, including: Anti Analysis, Antivirus, YARA, Data Collection, Defense Evasion, and Masquerade. Within each Category, there can be as many as 20 or 30 individual VTIs.

For many VTIs, there is even one deeper level of detail – the Technique. These are more specific strategies used by VTIs to identify threatening behavior. For each technique, a wide variety of scoring for each VTI can be customized, such as the Default Score which is set to 2 for all three of the techniques below:

Anti Analysis

31 Techniques

Makes analysis more challenging by detection and bypass of sandboxes, debuggers or other reverse engineering tools.

>> Tries to detect debugger

>> Tries to evade debugger

⌵ Tries to detect virtual machine

Technique	Built-in	Default Score	Documents Score	Scripts Score	Browser Score	MSI Score	Static Analysis Score	Enabled
Detects VM by file.	Yes	Def (2)	Def (4)	Def (4)	Def (4)	Def (2)	Def (Disabled)	<input checked="" type="checkbox"/>
Detects VM by module.	Yes	Def (2)	Def (4)	Def (4)	Def (4)	Def (2)	Def (Disabled)	<input checked="" type="checkbox"/>
Detects VM via rdtsc.	Yes	Def (2)	Def (4)	Def (4)	Def (4)	Def (2)	Def (Disabled)	<input checked="" type="checkbox"/>

Expand your Toolset with the IDA Pro Plugin

Use this Plugin to enrich IDA Pro static analysis with behavior-based data from VMRay. This speeds up in-depth analysis of malware threats by adding comments to dynamically resolved API calls within IDA, showing the resolved function, its parameters, return value and timestamp.

This Plugin also allows analysts to work more immediately and directly with smart memory dumps, which reveal far more information about malware behavior than static analysis alone can provide. It also streamlines tedious aspects of deep-dive analysis such as unpacking, de-obfuscating, and organizing malware files and runtime artifacts such as memory dumps

Address	Function	Instruction
region_952:005303DF	sub_530370	call [ebp+var_20] ; VMRay:
region_952:005303E9	sub_530370	call [ebp+var_20] ; VMRay:
region_952:00530560	sub_530540	call [ebp+var_C] ; VMRay:
region_952:00530593	sub_530570	call [ebp+var_C] ; VMRay:
region_952:00533526	sub_5334B4	call [ebp+var_4C] ; VMRay:
region_952:00533533	sub_5334B4	call [ebp+var_4C] ; VMRay:
region_952:00533888	sub_533894	call [ebp+var_4] ; VMRay:
region_952:005338F8	sub_5338C4	call [ebp+var_C] ; VMRay:
region_952:00533945	sub_533914	call [ebp+var_8] ; VMRay:
region_952:0053397D	sub_533954	call [ebp+var_8] ; VMRay:
region_952:005339D9	sub_533994	call [ebp+var_C] ; VMRay:
region_952:00533A19	sub_5339F4	call [ebp+var_8] ; VMRay:
region_952:00533A65	sub_533A34	call [ebp+var_C] ; VMRay:
region_952:00533AA5	sub_533A74	call [ebp+var_8] ; VMRay:
region_952:00533AD9	sub_533AB4	call [ebp+var_8] ; VMRay:
region_952:00533B15	sub_533AF4	call [ebp+var_8] ; VMRay:
region_952:00533B44	sub_533B24	call [ebp+var_C] ; VMRay:
region_952:00533B77	sub_533B54	call [ebp+var_C] ; VMRay:
region_952:00533C0D	sub_533BF4	call [ebp+var_C] ; VMRay:



16

of Fortune 100
Largest Companies



17

of the World's 100
Most Valuable Brands



4 of 5

World's Top 5
Tech Giants



37

Leading Finance
Organizations



56

Government
Customers



30

Countries
from All Regions

At VMRay, our purpose is to liberate the world from **undetectable digital threats**.

Led by reputable cyber security pioneers, we develop best-of-breed technologies to detect unknown threats that others miss. Thus, we empower organizations to **augment and automate** security operations by providing the world's best threat detection and analysis platform.

Contact Us

Email: sales@vmray.com
Phone: +1 888 958-5801

VMRay GmbH

Universitätsstraße 142
44799 Bochum • Germany

VMRay Inc.

22 Boston Wharf Road, 7th Floor
Boston, MA 02210 • USA

