ThreatGRID®
Malware Analysis & Threat Intelligence

EnCase® FACT SHEET

ThreatGRID® Malware Analysis & Intelligence For EnCase®

USE THREATGRID TO GAIN FULL INSIGHT INTO UNKNOWN THREATS IDENTIFIED BY ENCASE—WITH A RIGHT-CLICK

Gain deep insight into unknown threats identified by EnCase products. ThreatGRID provides deep, dynamic and static analysis of malware with full context—within minutes.

Visualize ThreatGRID analysis results. View ThreatGRID's Threat Score in the EnCase Enterprise interface—fully integrated.

Be proactive and improve your security. Download insightful malware analysis reports and detailed analysis JSON files from ThreatGRID.

ENCASE ENTERPRISE: NETWORK-ENABLED INCIDENT RESPONSE

Guidance Software is recognized worldwide as the industry leader in digital investigative solutions. Its EnCase® Enterprise platform is used by numerous government agencies, more than 65 percent of the Fortune 100, and more than 40 percent of the Fortune 500, to conduct digital investigations of servers, laptops, desktops and mobile devices.

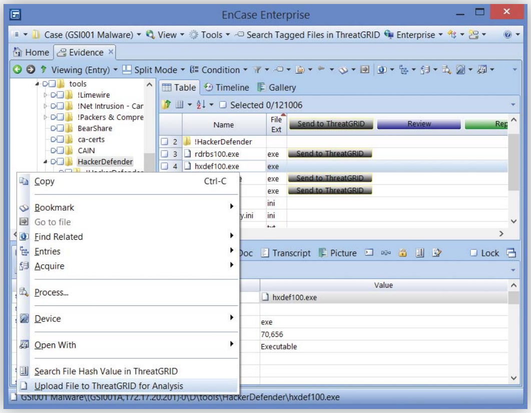
Built on the EnCase Enterprise platform are market-leading electronic discovery and cyber security solutions, EnCase® Cybersecurity and EnCase® Analytics. They empower organizations to perform sensitive data discovery for compliance purposes, conduct speedy and thorough security incident response, and reveal previously hidden advanced persistent threats or malicious insider activity.

THREATGRID ADVANCED MALWARE ANALYSIS

ThreatGRID is the first unified malware analysis and threat intelligence solution, that's revolutionizing how organizations use accurate and context-rich intelligence to better defend against targeted and advanced cyber attacks.

ThreatGRID securely crowdsources large volumes of malware and performs advanced analysis in the cloud, to identify key behavioral indicators enabling near real-time remediation. ThreatGRID provides full global context to help operators understand the attack metrics and whether other organizations were also affected. ThreatGRID also provides behavioral indicators and Threat Scores so analysts may quickly prioritize incidents and download detailed information and reports to better prepare against future attacks. ThreatGRID's API simplifies sample submission and intelligence integration with EnCase to maximize the effectiveness of the existing security infrastructure.

After EnCase Cybersecurity or EnCase Analytics has identified an unknown threat on an endpoint with the EnCase Enterprise platform, ThreatGRID provides in-depth analysis and correlates the attack-related artifacts with all other known malicious activities to help analysts quickly investigate and determine if malware resides in other parts of the network or if the incident should be closed.



ThreatGRID analysis from inside EnCase Enterprise.

THREATGRID + ENCASE: SAMPLE SCENARIO

Quick analysis results with one click

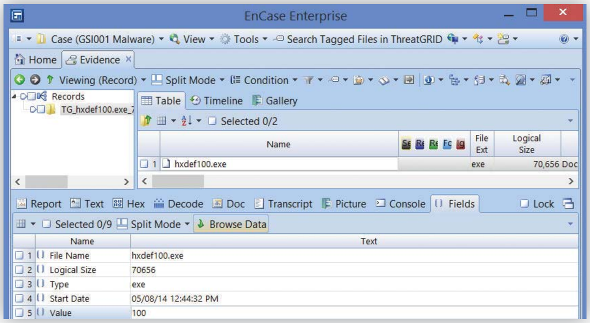
After EnCase has identified an unknown threat, the operator simply right-clicks on the file to automatically query ThreatGRID[1] for multiple forensic indicators gathered during the virtual infection.

[1] Subscription required for additional volumes.

Interested in trying our solution for yourself? Request a demo at **www.threatgrid.com/encase**

Information describing when the related sample was analyzed and its Threat Score are displayed in the EnCase Records tab. The Threat Score is in the Value field and indicates the severity and confidence levels of the sample based upon its unique behavioral indicators (no malware signatures required). ThreatGRID downloads the full analysis report for the suspected malware along with the path in the Location field. If the sample has never been analyzed, the same right-click function will allow the analyst to submit the File to ThreatGRID for analysis. Integrated investigative functions include:

- Search Highlighted IP Address, Highlighted Domain, File Hash Value and Tagged File Hash Values in ThreatGRID
- Upload File to ThreatGRID for Analysis



	Name	File Ext	Logical Size
1	hxdef100.exe	exe	70,656 Doc

	Name	Text
1	File Name	hxdef100.exe
2	Logical Size	70656
3	Type	exe
4	Start Date	05/08/14 12:44:32 PM
5	Value	100

In the EnCase Records tab, click on the Fields tab to see matched analysis results.

Detailed analysis in ThreatGRID

If the initial result requires further investigation, the detailed analysis results in the ThreatGRID portal are available for additional review. The ThreatGRID workflow menu options allow you to pivot to various sections of the report and extract artifacts of interest from the ThreatGRID portal.

Analyze network activity

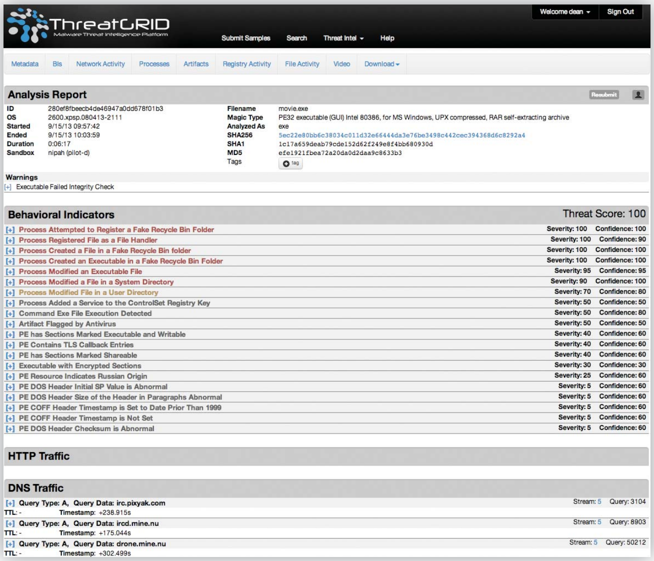
If applicable, detailed network communications of the malware is displayed. For example, determining the exact URL paths of HTTP-based C2 activity including a highly suspect User-Agent string is possible using ThreatGRID's network analysis.

Pivot and correlate for the big picture

ThreatGRID correlates samples based on multiple artifacts, each of which provides pivot points for analysts to see the full context of a threat and identify related samples in ThreatGRID's enormous global content repository. For example, pivoting on the IP Address and Domain yields additional details, including all other connected samples.

Download analysis results

Analysts may download all analysis objects such as disk and registry artifacts as well as full network packet captures for each submission from the ThreatGRID portal for detailed offline review.



Analysis Report

ID	280ef8fbeecb4de46947a0dd678f01b3	Filename	movie.exe
OS	2600.xpsp.080413-2111	Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed, RAR self-extracting archive
Started	9/15/13 09:57:42	Analyzed As	exe
Ended	9/15/13 10:03:59	SHA256	5ec22e80bb6c38034c011d32e66444da3e76be3498c442cec394368d6c8292a4
Duration	0:06:17	SHA1	1c17a659deab79cde152d62f249e8f4bb680930d
Sandbox	nipah (pilot-d)	MD5	efe1921fbea72a20da0d2daa9c8633b3
		Tags	

Warnings

[+] Executable Failed Integrity Check

Behavioral Indicators — Threat Score: 100

[+] Process Attempted to Register a Fake Recycle Bin Folder	Severity: 100	Confidence: 100
[+] Process Registered File as a File Handler	Severity: 100	Confidence: 90
[+] Process Created a File in a Fake Recycle Bin folder	Severity: 100	Confidence: 100
[+] Process Created an Executable in a Fake Recycle Bin Folder	Severity: 100	Confidence: 100
[+] Process Modified an Executable File	Severity: 95	Confidence: 95
[+] Process Modified a File in a System Directory	Severity: 90	Confidence: 100
[+] Process Modified File in a User Directory	Severity: 70	Confidence: 80
[+] Process Added a Service to the ControlSet Registry Key	Severity: 50	Confidence: 50
[+] Command Exe File Execution Detected	Severity: 50	Confidence: 80
[+] Artifact Flagged by Antivirus	Severity: 50	Confidence: 50
[+] PE has Sections Marked Executable and Writable	Severity: 40	Confidence: 60
[+] PE Contains TLS Callback Entries	Severity: 40	Confidence: 60
[+] PE has Sections Marked Shareable	Severity: 40	Confidence: 60
[+] Executable with Encrypted Sections	Severity: 30	Confidence: 30
[+] PE Resource Indicates Russian Origin	Severity: 25	Confidence: 60
[+] PE DOS Header Initial SP Value is Abnormal	Severity: 5	Confidence: 60
[+] PE DOS Header Size of the Header in Paragraphs Abnormal	Severity: 5	Confidence: 60
[+] PE COFF Header Timestamp is Set to Date Prior Than 1999	Severity: 5	Confidence: 60
[+] PE COFF Header Timestamp is Not Set	Severity: 5	Confidence: 60
[+] PE DOS Header Checksum is Abnormal	Severity: 5	Confidence: 60

HTTP Traffic

DNS Traffic

[+] Query Type: A, Query Data: irc.pixyak.com TTL: - Timestamp: +238.915s	Stream: 5	Query: 3104
[+] Query Type: A, Query Data: ircd.mine.nu TTL: - Timestamp: +175.044s	Stream: 5	Query: 8903
[+] Query Type: A, Query Data: drone.mine.nu TTL: - Timestamp: +302.499s	Stream: 5	Query: 50212

Detailed ThreatGRID analysis reports and JSON files, are also downloadable.

Free ThreatGRID Trial for EnCase Users

ThreatGRID Malware Analysis and Intelligence for EnCase is available for download at no cost from the EnCase App Central Store. As an EnCase user, contact encasesales@threatgrid.com for your free 30-day trial of ThreatGRID.

About ThreatGRID

ThreatGRID is the first unified malware analysis and threat intelligence solution that is revolutionizing how organizations use accurate and context-rich intelligence to defend against advanced cyber attacks. ThreatGRID empowers security teams to respond more quickly and effectively while increasing the value of their existing security investments. Founded by a team of security entrepreneurs with solid track records in the security software industry, ThreatGRID is a private company based in New York City.

ThreatGRID®
Malware Analysis & Threat Intelligence

ThreatGRID Inc.,
489 5th Avenue,
31st Floor
New York, NY 10017

Email: **encasesales@threatgrid.com**
Web: **www.threatgrid.com**
Twitter: **www.twitter.com/ThreatGRID**
LinkedIn: **www.linkedin.com/company/threatgrid-inc**