

INTEZER ANALYSES



INTEZER -

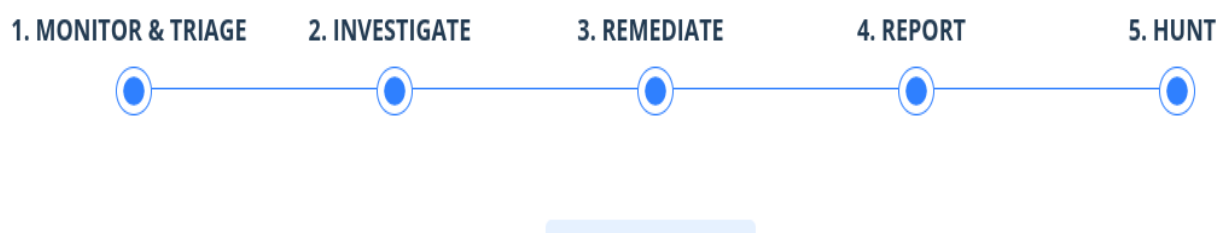
Intezer is “**innovating threat detection and response by mapping the genetic origins of software**”. Unlike traditional anomaly-based detection approaches, Intezer detects threats by identifying their code origins, resulting in fewer false positives and deep context for an effective response.

INTEZER ANALYSES -

Intezer automates alert triage, incident response and threat hunting by analyzing potential threats (such as files, URLs, endpoints) and automatically extracts IoCs/hunting rules—providing clear classification and better detection opportunities.

Working -

How it Works



1. Monitor & triage alerts -

- 4/7 monitoring and collection of endpoint and email security alerts.
- Deep analysis for any artifact (file, process, URL) related to the alert.
- Behavioral analysis for fileless commands (LOTL).
- Identify and close false positives.

2. Investigate -

- Deep memory & forensic analysis for suspected endpoints.
- Extract actionable IOCs and hunting rules.
- Cluster threats by threat actors and families.
- On-demand assistance from threat analysis expert.

3. Remediate -

- Get clear findings and recommended actions for all your alerts.
- Auto-remediate alerts and apply IOCs/rules according to your policy.
- Auto-hunt for additional infections based on IOCs and rules.

4. Report -

- Escalate serious incidents to your team by email to an emergency inbox.
- Dashboard for real-time visibility into your triage, response & hunting processes.
- Monthly executive report with key metrics about your alert triage and response process.

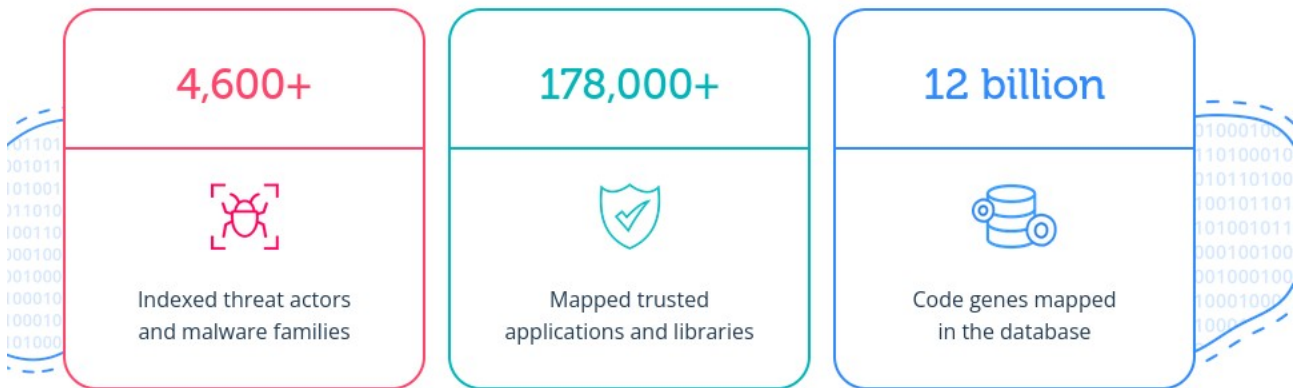
5. Proactive Hunting -

- Ongoing feeds of new detection opportunities seen in the wild for selected threat actors and malware families.
- Generate hunting rules easily for both families and individual threats.

What Makes Intezer Different

Every alert is automatically investigated and triaged by Intezer at a reverse-engineer level using transparent technology you can trust to avoid the risks of human errors or inconsistent results.

Intezer provides teams with a cost-effective platform that's easy to set up, so you can reduce your reliance on expensive outsourced SOC services.



Examples presented with Petiya golden eye builder :-

1) Accelerate EDR Alert Triage and Investigation

- Eliminate time spent on false positives from your endpoint security solution, while enriching and investigating alerts to confirm, prioritize, and kickstart incident response.

The screenshot displays the Intezer Analyze web interface. The top navigation bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and Live Classes. The main header shows the file being analyzed: 'Petya and GoldenEye BUILDER.exe' (258.5 KB). The interface is divided into several sections:

- Original File:** Shows the file name, size, and a 'Malicious' status with 'Generic Malware (17 Genes)'.
- Dynamic Execution:** A section for analyzing the file's behavior during execution.
- Static Extraction:** A section for analyzing the file's static components.
- Genetic Summary:** A central section showing the file's genetic makeup, including 'Generic Malware' (85.67%), 'IntelliLock' (1.67%), and 'VMProtect' (1.67%).
- File Metadata:** A table at the bottom providing detailed information about the file, including its size, SHA256 hash, MD5 hash, product name, file type, SHA1 hash, SSdeep hash, and target machine.

The bottom of the interface features a cookie notice and a 'Help' button.

46 / 65

46 security vendors and no sandboxes flagged this file as malicious

b4e9d14e4ea8a1c459805ec4687012a3e6a330864511a3d9c7af9b841403

PurgeRansomware.exe

24.00 KB
Size

2022-08-01 16:28:57 UTC
4 months ago

EXE

peexe assembly direct-ipc-clock-access detect-debug-environment runtime-modules

Community Score

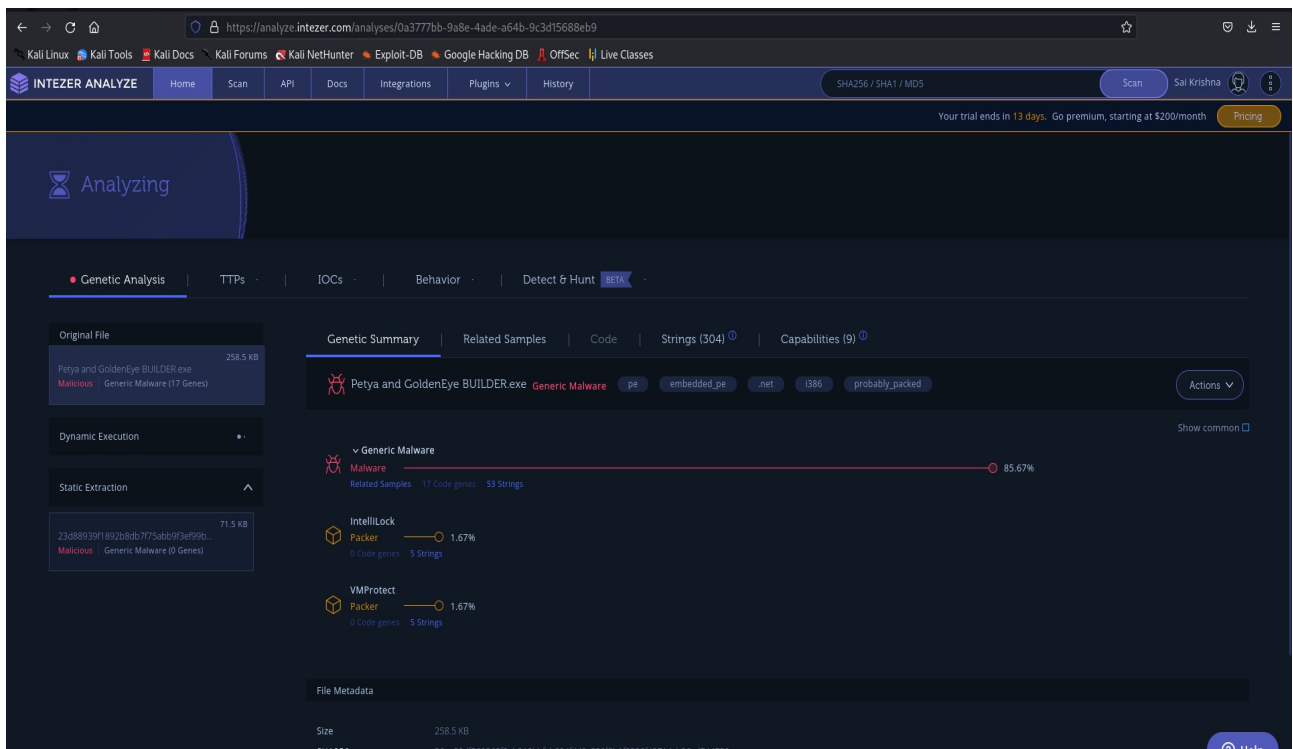
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security Vendors' Analysis

Ad-Aware	GenHeur.Ransom.MSIL.Idopl.1	AviLab-V3	Trojan.Win32.RL.Agent.C4136724
Alibaba	Ransom.MSIL.Cryptolite.25c3075	ALYac	Trojan.Ransom.Globe
Antiy-AVL	Trojan.Generic.ASMalware.SCS4	Avast	Win32.Malware-gen
AVG	Win32.Malware-gen	BitDefender	GenHeur.Ransom.MSIL.Idopl.1
BitDefenderTheta	Gen.NV.Zemaitis.34806.bm0@ax1uhgp	Comodo	Malware@kamjudy52b63
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cyberason	Malicious.5c5215
D-Web	Trojan.Encoder.13056	Elastic	Malicious (moderate Confidence)
Emisoft	GenHeur.Ransom.MSIL.Idopl.1 (B)	eScan	GenHeur.Ransom.MSIL.Idopl.1
ESET-NOD32	A Variant Of MSIL.Filecoder.FG	Furinet	MSIL.Filecoder.FG/ransom
GData	MSIL.Trojan-Ransom.FTSCoder.B	Gridinsoft (no cloud)	Malware.Win32.Gen.smlst1
Ikarus	Trojan-Ransom.MikeYan	Jiangmin	Trojan.MSIL.gikus
K7AntiVirus	Trojan (005086d1)	K7GW	Trojan (005086d1)
Kaspersky	Trojan-Ransom.MSIL.Agent.xi	MAX	Malware (ai.Score=100)

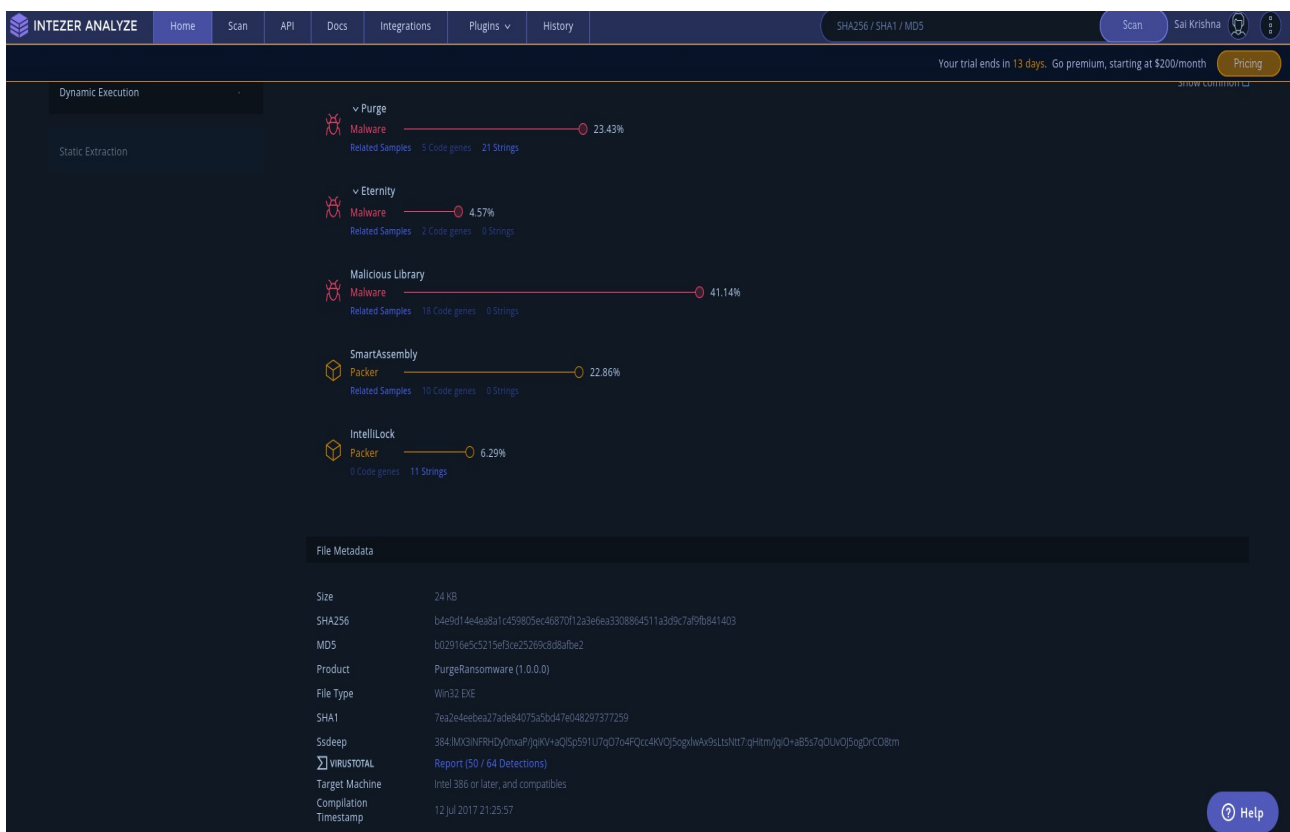
2) Automation for Phishing Investigation Pipelines -

- Automatically scan and extract IOCs from URLs and suspicious files to efficiently manage a high volume of phishing alerts.
- Integrate Intezer's automation into your abuse inbox or email security system to automatically classify file attachments or URLs and accelerate incident response.
- Intezer Analyze also provides a code-based vaccine for each threat which can be downloaded in several formats, including **YARA**, **STIX**, **Stix2**, and **OpenIOX**.
- Signatures that are based on code are stronger than string-based signatures because they are produced from the specific code that executes a certain functionality in the malware. You can use the vaccine and the information provided in the IoCs and TTPs tabs to detect similar files in the environment using your existing security tools like SIEM, EDR and XDR.



3) Advanced Incident Response Toolset for Analysts

- Go beyond traditional sandboxing with a single platform that provides file, memory, URL, and live endpoint scanning, plus reverse engineering capabilities.
- Reduce time spent on malware analysis tasks and switching between tools, while providing your team with a private database that logs data from every investigation.



INTEZER ANALYZE

HomeScanAPIDocsIntegrationsPlugins▼History

SHA256 / SHA1 / MD5

Scan

Sai Krishna

Your trial ends in 13 days. Go premium, starting at \$200/month

Pricing

Malicious

Main Family: Purge >

.NET Purge.exe

SHA256b4e9d14e4ea8a1c459805ec46870f12a3e6ea3308864511a3d9c7af9fb841403

Report (50 / 64 Detections)

pe .net i386 SmartAssembly

Known Malicious ⓘ

This file is a known malware and exists in Intezer's blacklist or is recognized by trusted security vendors

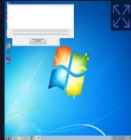
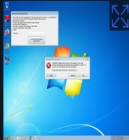

Actions ▼

Contact our Experts

Analyzed on Dec 23rd 2022

Genetic Analysis | TTPs | IOCs | Behavior | Detect & Hunt BETA | Extended Dynamic Execution

Screenshots



Process Tree

<ANALYZED-FILE-NAME>
pid 1852 | "C:\Users\<USER>\AppData\Local\Temp\<ANALYZED-FILE-NAME>" undefined

Network Activity

No Network Activity

Service Activity

No Service Activity

Help

INTEZER ANALYZE

HomeScanAPIDocsIntegrationsPlugins▼History

SHA256 / SHA1 / MD5

Scan

Sai Krishna

Your trial ends in 13 days. Go premium, starting at \$200/month

Pricing

Genetic Analysis | TTPs | IOCs | Behavior | Detect & Hunt BETA | Extended Dynamic Execution

Activity-based (7) | File-based (1)

Search...

Filters

Artifact Effectiveness ⓘ

▲ (0)

▲ (0)

▲ (7)

Artifact Type Filter

☒ All

☐ File Read (4)

☐ md5 (1)

☐ sha1 (1)

☐ sha256 (1)

Family Filter

☒ All

☐ Purge (7)

Activity-based Detection Opps

Ideal for creating SIEM and EDR rules ⓘ SIGMA

Extract Rules ▼

Download CSV

Artifact Type ▼	Artifact	Source	Seen In ⓘ	Related Samples ⓘ
<input type="checkbox"/> ▲ File Read	C:\Windows\system32\PurgeRansomware.pdb ⓘ	File Activity	Purge >	Related Samples
<input type="checkbox"/> ▲ sha1	7ea2e4eebea27ade84075a3bd47e048297377250 ⓘ	File	Purge >	Related Samples
<input type="checkbox"/> ▲ File Read	C:\Users\<USER>\AppData\Local\Temp\PurgeRansomware.pdb ⓘ	File Activity	Purge >	Related Samples
<input type="checkbox"/> ▲ sha256	b4e9d14e4ea8a1c459805ec46870f12a3e6ea3308864511a3d9c7af9fb841403 ⓘ	File	Purge >	Related Samples
<input type="checkbox"/> ▲ File Read	C:\Windows\system32\PurgeRansomware.pdb ⓘ	File Activity	Purge >	Related Samples
<input type="checkbox"/> ▲ md5	b02916e5c5215e3ce25269c8d8afce2 ⓘ	File	Purge >	Related Samples
<input type="checkbox"/> ▲ File Read	C:\Windows\PurgeRansomware.pdb ⓘ	File Activity	Purge >	Related Samples

Help

4) Expand Your Proactive Threat Hunting Capabilities -

- Explore and track threats based on your needs, with extracted IoCs, TTPs, and advanced detection opportunities to hunt for infections and create detection rules.
- Stay ahead of attackers by proactively hunting for advanced threats based on the threat actors and malware families that you are tracking.

The screenshot displays the Intezer Analyze web application interface. The browser address bar shows the URL <https://analyze.intezer.com/analyses/689908f2-2990-470c-95e4-b32d60892ef2/detect-hunt>. The page features a navigation bar with tabs for Home, Scan, API, Docs, Integrations, Plugins, and History. A search bar and a 'Scan' button are visible, along with a user profile for 'Sai Krishna'. A trial notice indicates 'Your trial ends in 13 days. Go premium, starting at \$200/month'. The main content area is titled 'Activity-based (25) | File-based (9)' and 'Activity-based Detection Opps'. It includes a search bar, filters, and a table of detection opportunities. The table columns are Artifact Type, Artifact, Source, Seen In, and Related Samples. The artifacts listed include network activity from baroqueetes.com, registry writes to various system locations, and file activities in the Windows system directory and ProgramData. A pyramid diagram on the left shows artifact effectiveness levels (0, 18, 7). The bottom left shows filters for Artifact Type (All, File Write, Network, Process Command, Registry Write, File Read, md5, sha1, sha256) and Family (All, DarkSide Ransomware, Malicious Library).

Artifact Type	Artifact	Source	Seen In	Related Samples
Network	baroqueetes.com:103.224.182.242	Network Activity	DarkSide Ransomware	Related Samples
Registry Write	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\c2c48c32\DefaultIcon	Registry Activity	DarkSide Ransomware	Related Samples
Registry Write	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\c2c48c32\Default	Registry Activity	DarkSide Ransomware	Related Samples
Registry Write	HKEY_CLASSES_ROOT\c2c48c32	Registry Activity	DarkSide Ransomware	Related Samples
Registry Write	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\c2c48c32\...	Registry Activity	DarkSide Ransomware	Related Samples
Registry Write	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\c2c48c32\...	Registry Activity	DarkSide Ransomware	Related Samples
File Write	C:\Windows\System32\config\systemprofile\AppData\Local\Mic...	File Activity	DarkSide Ransomware	Related Samples
File Write	C:\ProgramData\c2c48c32\ico	File Activity	DarkSide Ransomware	Related Samples
Network	baroqueetes.com	Network Activity	DarkSide Ransomware	Related Samples
Registry Write	HKEY_CLASSES_ROOT\c2c48c32\DefaultIcon	Registry Activity	DarkSide Ransomware	Related Samples

INTEZER ANALYZE

HomeScanAPIDocsIntegrationsPluginsHistory

SHA256 / SHA1 / MD5

Scan

Sai Krishna

Your trial ends in 13 days. Go premium, starting at \$200/month

Pricing

Actions

Infected Emotet

Scan Type: Live Memory Analysis
Scan Status: All processes were scanned
Analysis Time: 18:37 | 22.08.2022

OS Version: Windows 10
Scanner Version: 1.0.1.2

Loaded Modules

Scheduled Tasks

Search

Sort By: Verdict

Filters: Select

File name	Verdict	Family	Type	File path	Process name	Command line
cofirecofire.exe-Dx5290000	Malicious	Emotet	Injected module		cofirecofire.exe	
cofirecofire.exe	Malicious	Emotet	File system	c:\windows\systemow64\cofirecofire.exe	cofirecofire.exe	
cofirecofire.exe-Dx52b0000	Malicious	Emotet	Injected module		cofirecofire.exe	
catsrvps.dll	Trusted	Microsoft Visual C/C++ Libraries	File system	c:\windows\system32\catsrvps.dll	dllhost.exe	
catsrvut.dll	Trusted	Microsoft Corporation	File system	c:\windows\system32\catsrvut.dll	dllhost.exe	
catsrv.dll	Trusted	Microsoft Corporation	File system	c:\windows\system32\catsrv.dll	dllhost.exe	
wuaueng.dll	Trusted	Microsoft Corporation	File system	c:\windows\system32\wuaueng.dll	svchost.exe	
appxdeploymentclient.dll	Trusted	Microsoft Corporation	File system	c:\windows\system32\appxdeploymentclient.dll	svchost.exe	

Help

10 IOC IP Adress of Malicious Threats -

INTEZER ANALYZE

HomeScanAPIDocsIntegrationsPluginsHistory

SHA256 / SHA1 / MD5

Scan

Sai Krishna

Your trial ends in 13 days. Go premium, starting at \$200/month

Pricing

Type	IOC	Source Type	Classification
IP	107.160.120.122	Network communication	
IP	125.212.224.205	Network communication	
IP	151.101.66.159	Network communication	
IP	34.243.91.242	Network communication	
IP	34.149.87.45	Network communication	
IP	103.130.216.122	Network communication	
IP	185.53.179.173	Network communication	
IP	52.20.84.62	Network communication	
IP	34.102.136.180	Network communication	
IP	38.85.254.112	Network communication	
IP	52.128.23.153	Network communication	
IP	211.41.71.223	Network communication	
IP	173.232.203.98	Network communication	
Domain	www.qjgc.com	Network communication	

Help

