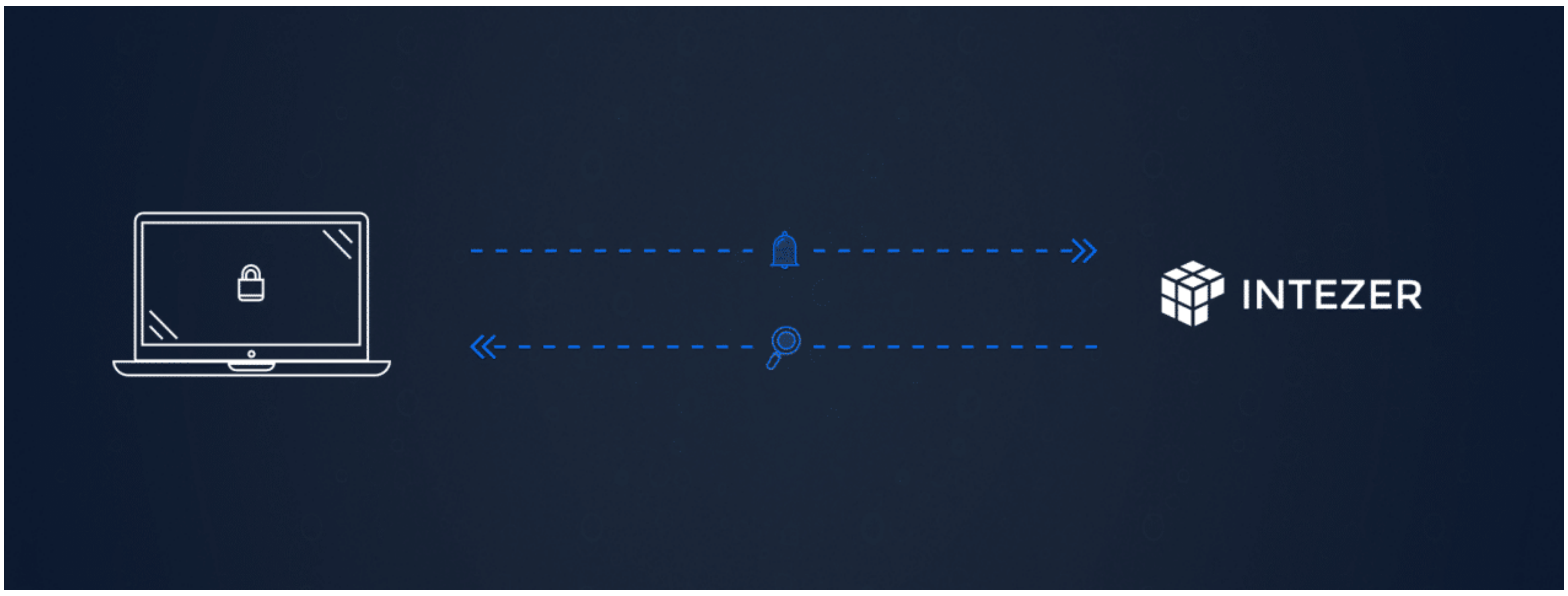
Automate Alert Triage and Response Tasks with Intezer EDR Connect

Written by Avigayil Mechtinger - 12 April 2022

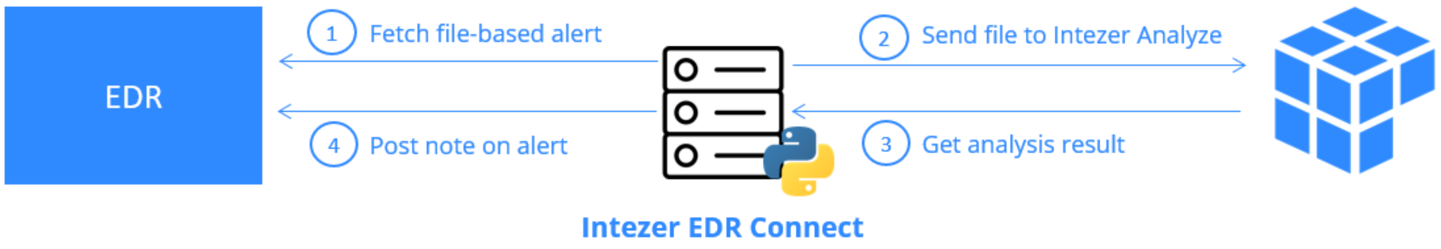


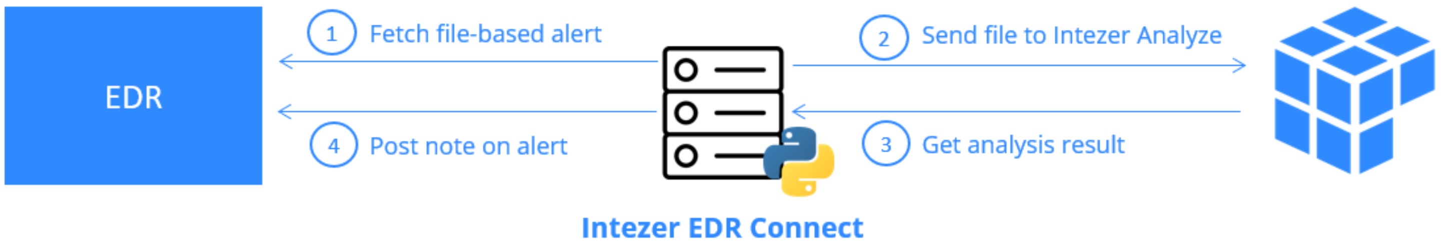
Integrate with SentinelOne, CrowdStrike, and More

One of the biggest pain points of cyber security teams is alert fatigue — trying to keep up with a tedious, never-ending stream of alerts to triage. In today’s reality, security teams spend a large amount of their valuable time on confirming alerts instead of investigating real incidents.

To tackle the alert fatigue most security teams experience and help improve MTTR (mean time to respond), we have developed Intezer EDR Connect. Intezer EDR Connect provides you with a lightweight and simple way to automate EDR alert triage. We use Intezer to enrich file-based alerts in your EDR and accelerate the investigation and prioritization processes.

In this post we will briefly overview the “journey” of an alert and explain how Intezer EDR Connect accelerates this journey.





The Journey of an Alert

From confirmation through prioritization and response.

Confirmation

In this step we will confirm that the alert is indeed a true-positive.

EDRs and other detection engines are designed to provide signals about suspicious behavior or anomalies in the context of the entity they are monitoring (endpoints, emails, etc.). These signals raise a high volume of alerts, and depending on your tuning and tooling, can contain a large percentage of low priority alerts or false positives.

As an example, the behavior of creating persistence can be seen in both malicious and legitimate software.

Recent study by Orange cyber defense shows that malware detection signals have doubled from 2020 to 2021. With organizations expanding their EDR deployments, the number of detection signals increases as well.

Overcoming false positives by turning off noisy signals or excluding directories that trigger noisy alerts is bad practice. Remember the SolarWinds cyberattack? SolarWinds advised excluding directories from anti-malware scanning to avoid false positives. Same directories that contained the malicious DLLs that were part of the attack.

Prioritization

For confirmed file-based incidents, knowing that the file is malicious is not enough. Malware attribution and classification is crucial for properly responding and prioritizing incident response.

As an example, let's say we have an alert of a backdoor and an alert of a coin miner. We will first respond to the backdoor alert, because it has a higher potential for damaging the organization. It can potentially deliver ransomware or steal classified information of customers or of the organization, whereas the CoinMiner can damage performance, which also has destructive potential, but probably less than a backdoor.

Incident Response

Creating detection and hunting rules are an essential part of cybersecurity teams' responsibilities. One of the first steps after confirming an incident and initiating the incident response process, is hunting for the existence of the threat in other endpoints inside the organization. Hunting for file hashes or basic network artifacts is not enough. They are short lived and can be easily manipulated. This applies also for creating detection rules and providing IoCs to summarize the incident, all of which are part of the incident response lifecycle.

Enriching alerts with detection opportunities helps security teams create quality and effective rules to better accomplish tasks within the incident response lifecycle.

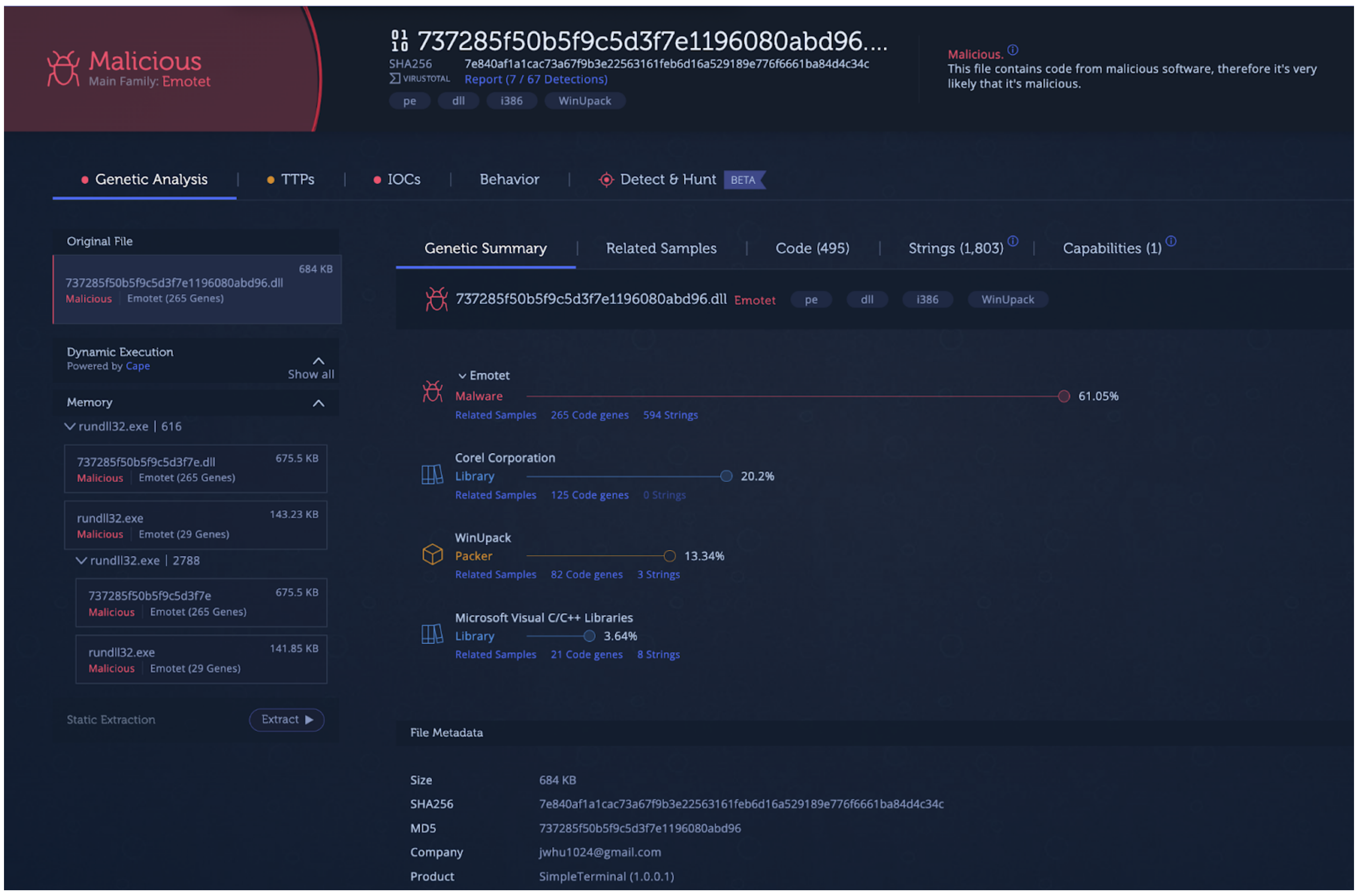
Use Intezer EDR Connect to Accelerate your Alert Journey

Intezer EDR connect integrates between your EDR and Intezer platform.

How Does it Work?

As shown in the diagram above, the connector fetches new file-based alerts from your EDR and sends them to analysis in Intezer. Then, the connector pushes the analysis result to the EDR as an incident note.

Intezer analyzes files using both static and dynamic techniques. It detonates the file in a sandbox, extracts memory modules, and compares the extracted code against an extensive code genome database. Intezer's unique code reuse detection technology allows you to determine the file verdict and its classification and origin. This capability enables you to confirm and prioritize alerts within seconds.



737285f50b5f9c5d3f7e1196080abd96....
SHA256 7e840af1a1cac73a67f9b3e22563161feb6d16a529189e776f6661ba84d4c34c
VIRUSTOTAL Report (7 / 67 Detections)

Malicious.
This file contains code from malicious software, therefore it's very likely that it's malicious.

Original File
737285f50b5f9c5d3f7e1196080abd96.dll 684 KB
Malicious | Emotet (265 Genes)

rundll32.exe | 616
737285f50b5f9c5d3f7e.dll 675.5 KB
Malicious | Emotet (265 Genes)
rundll32.exe 143.23 KB
Malicious | Emotet (29 Genes)
rundll32.exe | 2788
737285f50b5f9c5d3f7e 675.5 KB
Malicious | Emotet (265 Genes)
rundll32.exe 141.85 KB
Malicious | Emotet (29 Genes)

737285f50b5f9c5d3f7e1196080abd96.dll Emotet pe dll i386 WinUpack

Emotet
Malware 61.05%
Related Samples 265 Code genes 594 Strings

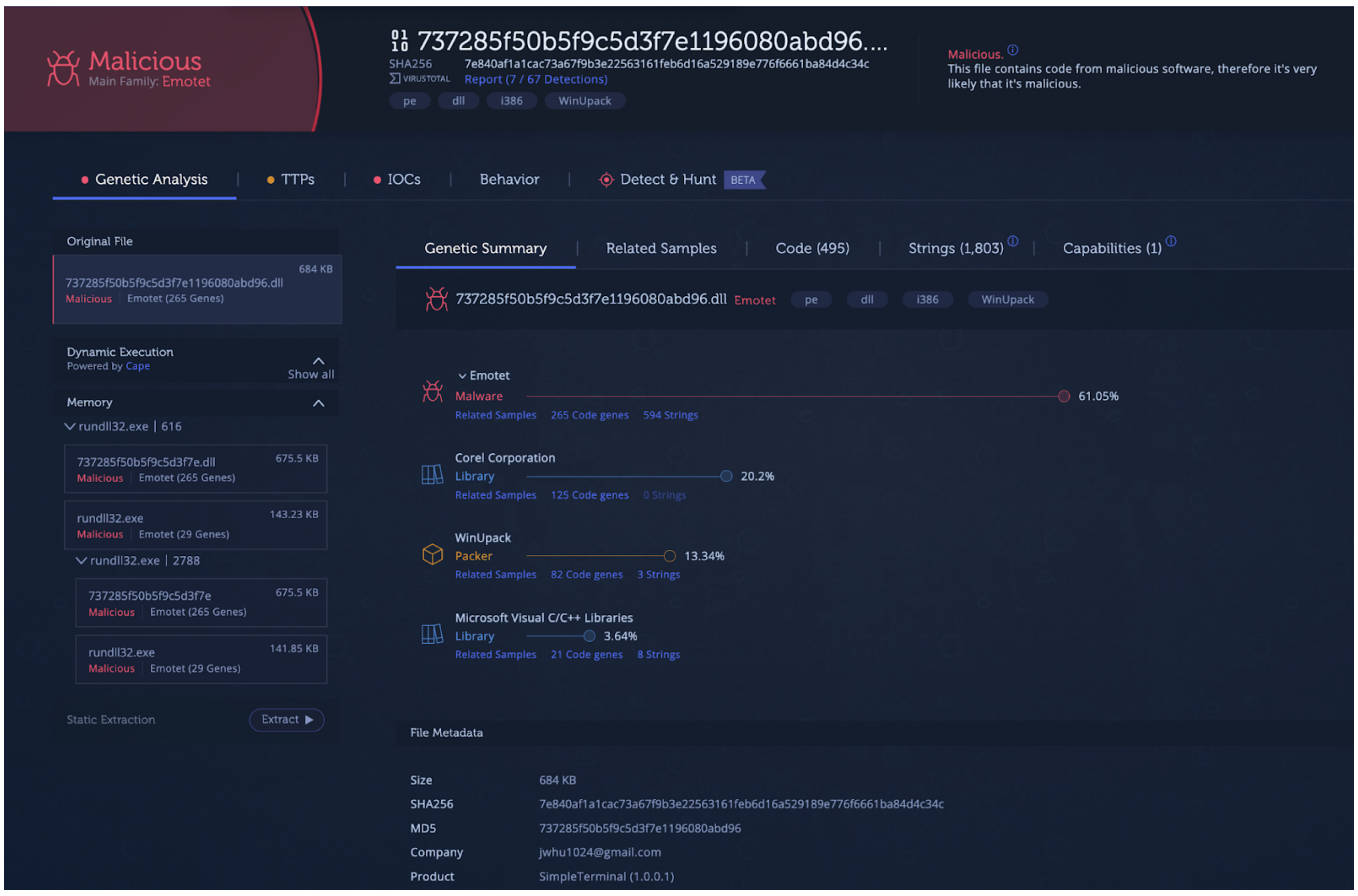
Corel Corporation
Library 20.2%
Related Samples 125 Code genes 0 Strings

WinUpack
Packer 13.34%
Related Samples 82 Code genes 3 Strings

Microsoft Visual C/C++ Libraries
Library 3.64%
Related Samples 21 Code genes 8 Strings

File Metadata

Size	684 KB
SHA256	7e840af1a1cac73a67f9b3e22563161feb6d16a529189e776f6661ba84d4c34c
MD5	737285f50b5f9c5d3f7e1196080abd96
Company	jwhu1024@gmail.com
Product	SimpleTerminal (1.0.0.1)



737285f50b5f9c5d3f7e1196080abd96....
SHA256 7e840af1a1cac73a67f9b3e22563161feb6d16a529189e776f6661ba84d4c34c
VIRUSTOTAL Report (7 / 67 Detections)

Malicious.
This file contains code from malicious software, therefore it's very likely that it's malicious.

Original File
737285f50b5f9c5d3f7e1196080abd96.dll 684 KB
Malicious | Emotet (265 Genes)

rundll32.exe | 616
737285f50b5f9c5d3f7e.dll 675.5 KB
Malicious | Emotet (265 Genes)
rundll32.exe 143.23 KB
Malicious | Emotet (29 Genes)
rundll32.exe | 2788
737285f50b5f9c5d3f7e 675.5 KB
Malicious | Emotet (265 Genes)
rundll32.exe 141.85 KB
Malicious | Emotet (29 Genes)

737285f50b5f9c5d3f7e1196080abd96.dll Emotet pe dll i386 WinUpack

Emotet
Malware 61.05%
Related Samples 265 Code genes 594 Strings

Corel Corporation
Library 20.2%
Related Samples 125 Code genes 0 Strings

WinUpack
Packer 13.34%
Related Samples 82 Code genes 3 Strings

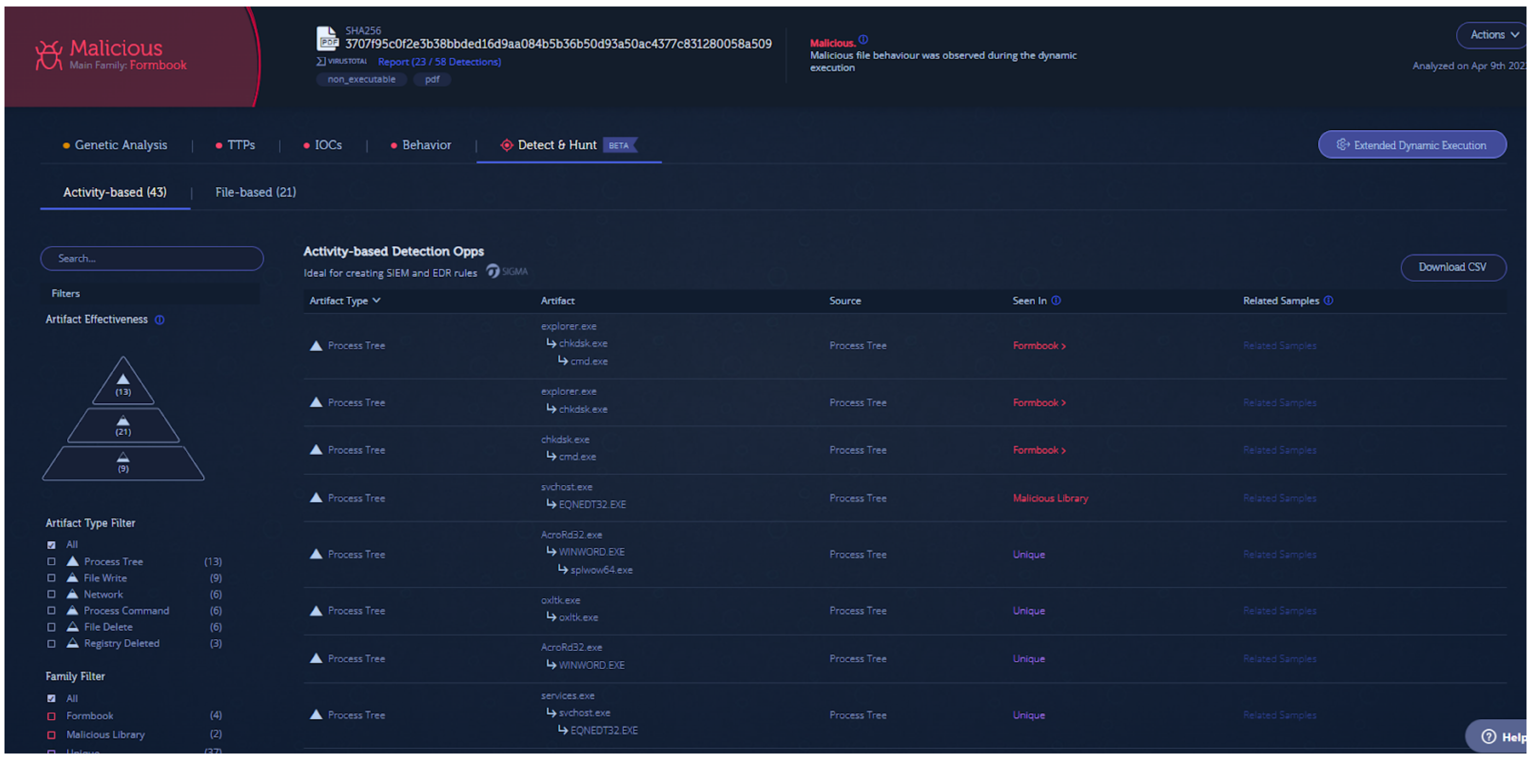
Microsoft Visual C/C++ Libraries
Library 3.64%
Related Samples 21 Code genes 8 Strings

File Metadata

Size	684 KB
SHA256	7e840af1a1cac73a67f9b3e22563161feb6d16a529189e776f6661ba84d4c34c
MD5	737285f50b5f9c5d3f7e1196080abd96
Company	jwhu1024@gmail.com
Product	SimpleTerminal (1.0.0.1)

Emotet example in Intezer analyze

To help you with the incident response process, investigation and quality rules creation within the entire incident response lifecycle, we have added the Detect & Hunt feature. Detect & Hunt combines our unique classification abilities with sandboxing, to present high-quality detection content. By matching the malware behavior against a huge database of malware and benign software behavior, we filter out non-relevant artifacts and present those that are unique to the studied sample or that have been previously seen in other malware samples. This allows analysts to quickly create effective rules, with high accuracy and low false-positive rate.



Malicious
Main Family: Formbook

SHA256
3707f95c0f2e3b38bbded16d9aa084b5b36b50d93a50ac4377c831280058a509
VIRUSTOTAL Report (23 / 58 Detections)
non_executable pdf

Malicious.
Malicious file behaviour was observed during the dynamic execution

Analyzed on Apr 9th 202

Actions
Genetic Analysis | TTPs | IOCs | Behavior | Detect & Hunt BETA
Extended Dynamic Execution
Activity-based (43) | File-based (21)
Search...

Filters

Artifact Effectiveness

Artifact Type Filter

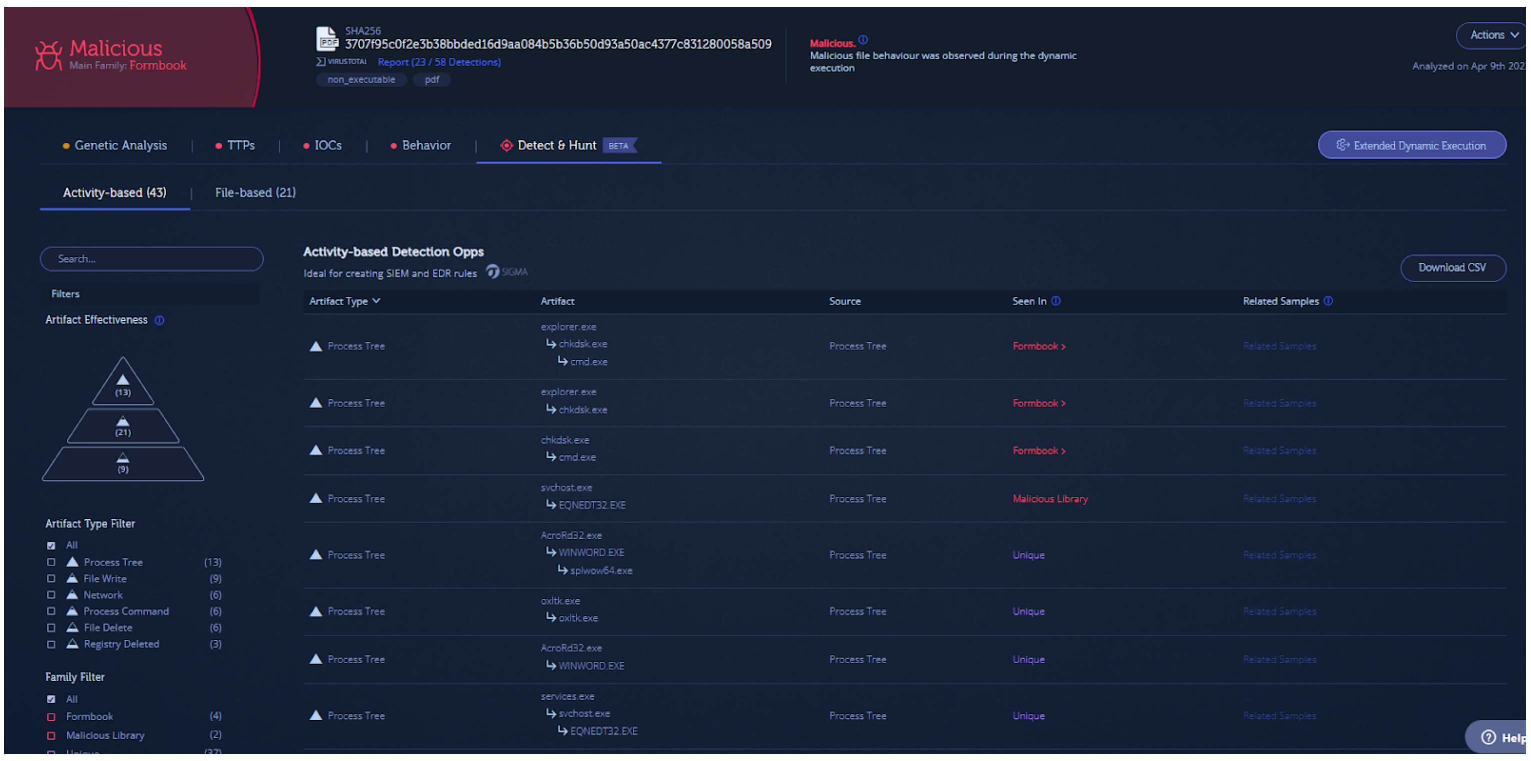
☑ All	
☐ Process Tree	(13)
☐ File Write	(9)
☐ Network	(6)
☐ Process Command	(6)
☐ File Delete	(6)
☐ Registry Deleted	(3)

Family Filter

☑ All	
☐ Formbook	(4)
☐ Malicious Library	(2)
☐ Unique	(37)

Activity-based Detection Opps
Ideal for creating SIEM and EDR rules SIGMA

Artifact Type	Artifact	Source	Seen In	Related Samples
Process Tree	explorer.exe ↳ chkdsk.exe ↳ cmd.exe	Process Tree	Formbook ›	Related Samples
Process Tree	explorer.exe ↳ chkdsk.exe	Process Tree	Formbook ›	Related Samples
Process Tree	chkdsk.exe ↳ cmd.exe	Process Tree	Formbook ›	Related Samples
Process Tree	svchost.exe ↳ EQNEDT32.EXE	Process Tree	Malicious Library	Related Samples
Process Tree	AcroRd32.exe ↳ WINWORD.EXE ↳ splwow64.exe	Process Tree	Unique	Related Samples
Process Tree	oxltk.exe ↳ oxltk.exe	Process Tree	Unique	Related Samples
Process Tree	AcroRd32.exe ↳ WINWORD.EXE	Process Tree	Unique	Related Samples
Process Tree	services.exe ↳ svchost.exe ↳ EQNEDT32.EXE	Process Tree	Unique	Related Samples



Malicious
Main Family: Formbook

SHA256
3707f95c0f2e3b38bbded16d9aa084b5b36b50d93a50ac4377c831280058a509
VIRUSTOTAL Report (23 / 58 Detections)
non_executable pdf

Malicious.
Malicious file behaviour was observed during the dynamic execution

Analyzed on Apr 9th 202

Filters

Artifact Effectiveness

Artifact Type Filter

☑ All	
☐ Process Tree	(13)
☐ File Write	(9)
☐ Network	(6)
☐ Process Command	(6)
☐ File Delete	(6)
☐ Registry Deleted	(3)

Family Filter

☑ All	
☐ Formbook	(4)
☐ Malicious Library	(2)
☐ Unique	(37)

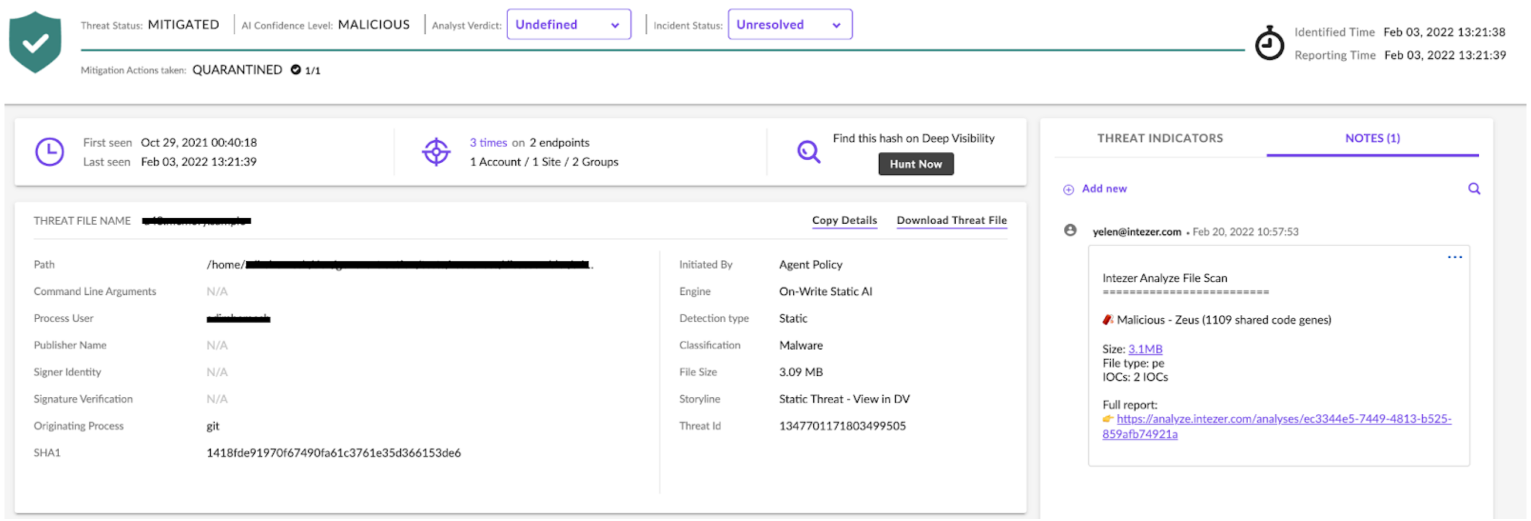
Activity-based Detection Opps
Ideal for creating SIEM and EDR rules SIGMA

Artifact Type	Artifact	Source	Seen In	Related Samples
Process Tree	explorer.exe ↳ chkdsk.exe ↳ cmd.exe	Process Tree	Formbook ›	Related Samples
Process Tree	explorer.exe ↳ chkdsk.exe	Process Tree	Formbook ›	Related Samples
Process Tree	chkdsk.exe ↳ cmd.exe	Process Tree	Formbook ›	Related Samples
Process Tree	svchost.exe ↳ EQNEDT32.EXE	Process Tree	Malicious Library	Related Samples
Process Tree	AcroRd32.exe ↳ WINWORD.EXE ↳ splwow64.exe	Process Tree	Unique	Related Samples
Process Tree	oxltk.exe ↳ oxltk.exe	Process Tree	Unique	Related Samples
Process Tree	AcroRd32.exe ↳ WINWORD.EXE	Process Tree	Unique	Related Samples
Process Tree	services.exe ↳ svchost.exe ↳ EQNEDT32.EXE	Process Tree	Unique	Related Samples

To read more about Detect & Hunt, browse to [Scale Incident Response with Detection Engineering: Intezer Detect & Hunt]().

Examples of Intezer-Enriched Alerts in EDRs

Example of an enriched incident in [SentinelOne](), with the analysis automatically added by Intezer EDR Connect noted on the right:



Threat Status: MITIGATED | AI Confidence Level: MALICIOUS | Analyst Verdict: Undefined | Incident Status: Unresolved

Mitigation Actions taken: QUARANTINED 1/1

Identified Time Feb 03, 2022 13:21:38
Reporting Time Feb 03, 2022 13:21:39

First seen Oct 29, 2021 00:40:18
Last seen Feb 03, 2022 13:21:39

3 times on 2 endpoints
1 Account / 1 Site / 2 Groups

Find this hash on Deep Visibility

THREAT FILE NAME [redacted]

Path	/home/[redacted].	Initiated By	Agent Policy
Command Line Arguments	N/A	Engine	On-Write Static AI
Process User	[redacted]	Detection type	Static
Publisher Name	N/A	Classification	Malware
Signer Identity	N/A	File Size	3.09 MB
Signature Verification	N/A	Storyline	Static Threat - View in DV
Originating Process	git	Threat Id	1347701171803499505
SHA1	1418fde91970f67490fa61c3761e35d366153de6		

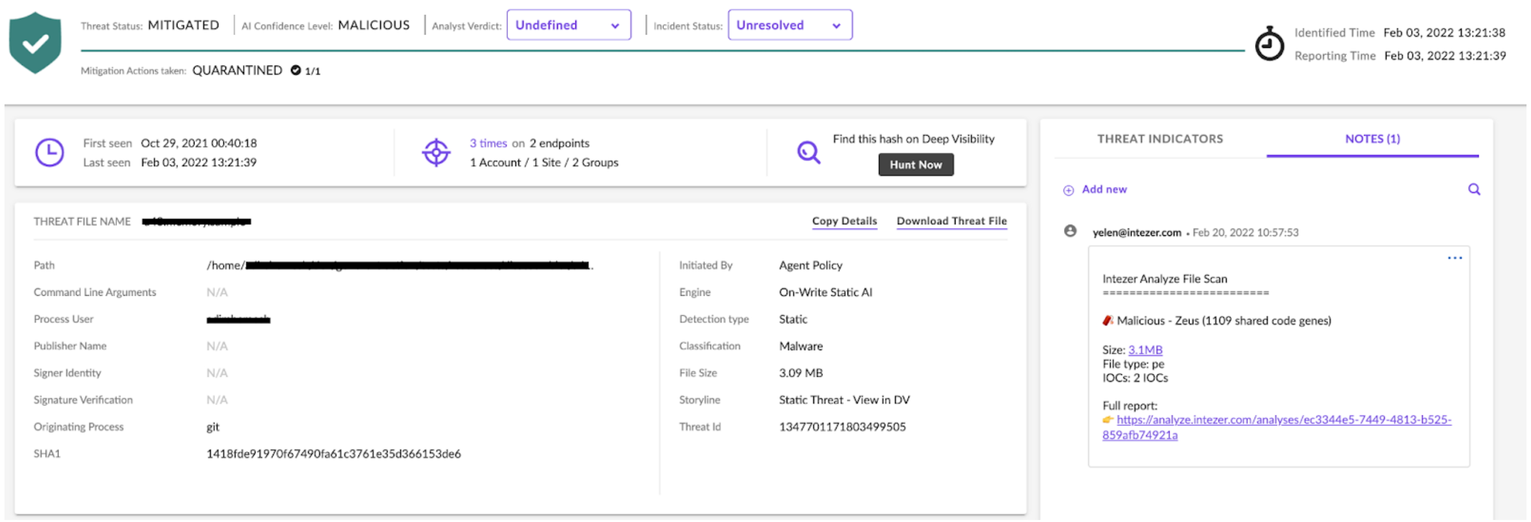
yelen@intezer.com • Feb 20, 2022 10:57:53

Intezer Analyze File Scan
========================

Malicious - Zeus (1109 shared code genes)

Size: 3.1MB
File type: pe
IOCs: 2 IOCs

Full report:
👉 https://analyze.intezer.com/analyses/ec3344e5-7449-4813-b525-859afb74921a



Threat Status: MITIGATED | AI Confidence Level: MALICIOUS | Analyst Verdict: Undefined | Incident Status: Unresolved

Mitigation Actions taken: QUARANTINED 1/1

Identified Time Feb 03, 2022 13:21:38
Reporting Time Feb 03, 2022 13:21:39

First seen Oct 29, 2021 00:40:18
Last seen Feb 03, 2022 13:21:39

3 times on 2 endpoints
1 Account / 1 Site / 2 Groups

Find this hash on Deep Visibility

THREAT FILE NAME [redacted]

Path	/home/[redacted].	Initiated By	Agent Policy
Command Line Arguments	N/A	Engine	On-Write Static AI
Process User	[redacted]	Detection type	Static
Publisher Name	N/A	Classification	Malware
Signer Identity	N/A	File Size	3.09 MB
Signature Verification	N/A	Storyline	Static Threat - View in DV
Originating Process	git	Threat Id	1347701171803499505
SHA1	1418fde91970f67490fa61c3761e35d366153de6		

yelen@intezer.com • Feb 20, 2022 10:57:53

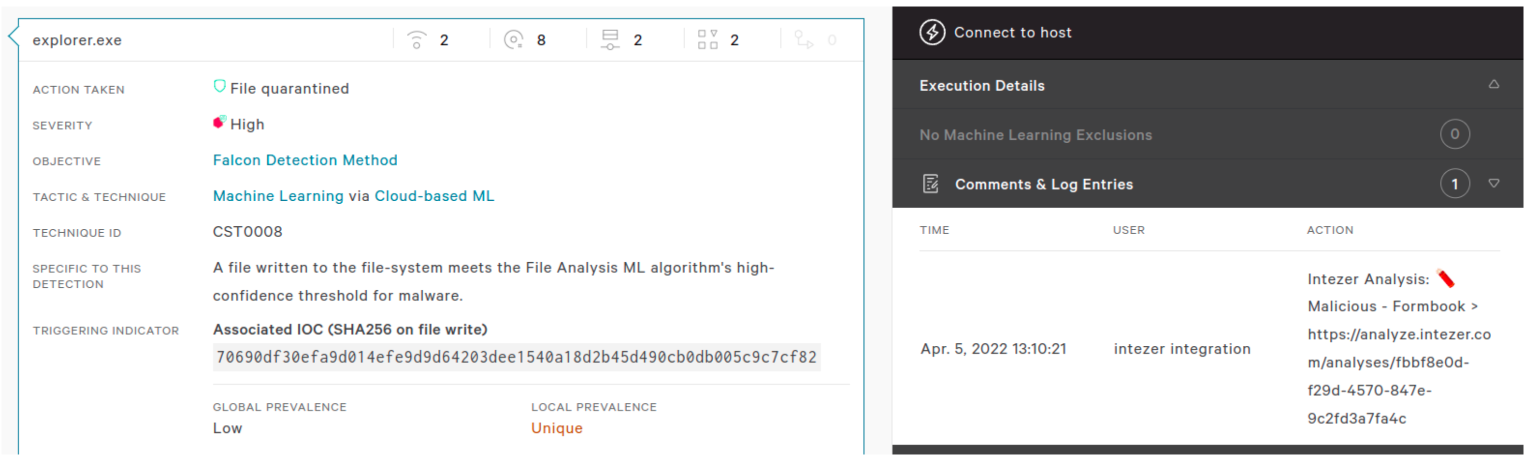
Intezer Analyze File Scan
========================

Malicious - Zeus (1109 shared code genes)

Size: 3.1MB
File type: pe
IOCs: 2 IOCs

Full report:
👉 https://analyze.intezer.com/analyses/ec3344e5-7449-4813-b525-859afb74921a

Example of an enriched incident in CrowdStrike:



explorer.exe

ACTION TAKEN: File quarantined

SEVERITY: High

OBJECTIVE: Falcon Detection Method

TACTIC & TECHNIQUE: Machine Learning via Cloud-based ML

TECHNIQUE ID: CST0008

SPECIFIC TO THIS DETECTION: A file written to the file-system meets the File Analysis ML algorithm's high-confidence threshold for malware.

TRIGGERING INDICATOR: Associated IOC (SHA256 on file write)
`70690df30efa9d014efe9d9d64203dee1540a18d2b45d490cb0db005c9c7cf82`

GLOBAL PREVALENCE: Low

LOCAL PREVALENCE: Unique

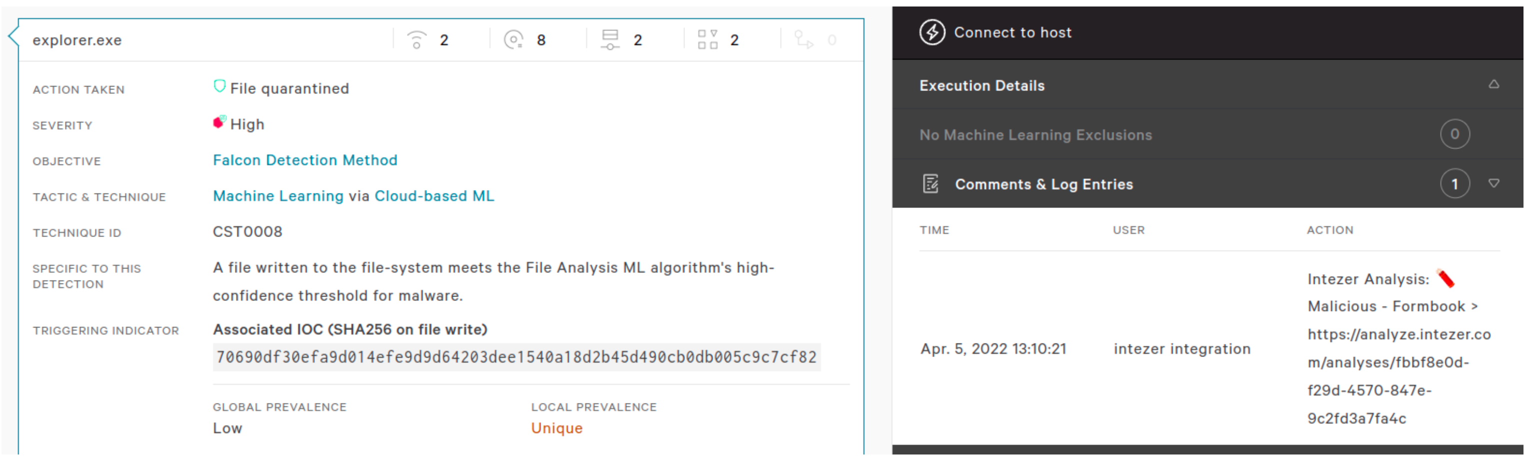
Connect to host

Execution Details

No Machine Learning Exclusions 0

Comments & Log Entries 1

TIME	USER	ACTION
Apr. 5, 2022 13:10:21	intezer integration	Intezer Analysis: Malicious - Formbook > https://analyze.intezer.com/analyses/fbbf8e0d-f29d-4570-847e-9c2fd3a7fa4c



explorer.exe

ACTION TAKEN: File quarantined

SEVERITY: High

OBJECTIVE: Falcon Detection Method

TACTIC & TECHNIQUE: Machine Learning via Cloud-based ML

TECHNIQUE ID: CST0008

SPECIFIC TO THIS DETECTION: A file written to the file-system meets the File Analysis ML algorithm's high-confidence threshold for malware.

TRIGGERING INDICATOR: Associated IOC (SHA256 on file write)
70690df30efa9d014efe9d9d64203dee1540a18d2b45d490cb0db005c9c7cf82

GLOBAL PREVALENCE: Low

LOCAL PREVALENCE: Unique

Connect to host

Execution Details

No Machine Learning Exclusions 0

Comments & Log Entries 1

TIME USER ACTION
Apr. 5, 2022 13:10:21 intezer integration Intezer Analysis: Malicious - Formbook > https://analyze.intezer.com/analyses/fbbf8e0d-f29d-4570-847e-9c2fd3a7fa4c

Upcoming EDR support

This connector supports SentinelOne and CrowdStrike, support for additional EDRs such as Microsoft Defender, Carbon Black, and more is coming soon. Contact us to learn more about upcoming EDR integrations.

Start Enriching your Alerts with Intezer

Intezer can host EDR Connect for enterprise users. For more information, please visit Intezer EDR Connect Docs or reach out to our team for a demo and to talk about upgrading your account.

Get a Demo

Avigayil Mechtinger

Avigayil is a product manager at Intezer, leading Intezer Analyze product lifecycle. Prior to this role, Avigayil was part of Intezer's research team and specialized in malware analysis and threat hunting. During her time at Intezer, she has uncovered and documented different malware targeting both Linux and Windows platforms.

Alert Triage Automation Incident Response Intezer Analyze Technology Integration Top blogs