TL;DR — You can now subscribe to threat actors/malware families in Intezer and receive notifications for new IoCs and detection opportunities.

Staying on top of emerging threats and keeping your detection rules on track is challenging. To keep track, security teams have to continuously go over different reports, from different sources, for various threats. On top of that, these reports usually provide low-pyramid IoCs (file hashes, IPs, and domains), leaving more effective and longer-lasting detection opportunities hidden.

To help you stay on top of emerging threats with the most updated detection rules, we have extended Intezer's threat family tracking:

- Intezer's Detect & Hunt feature is now available per threat family. While the Detect & Hunt tab has previously surfaced detection opportunities for a single file, now, it is possible to view aggregated IOCs/detection content for an entire threat actor or malware family. Detect & Hunt allows you to extract high-quality IoCs and detection content (to use in your SIEM or EDR), quickly and effectively. This saves you time and effort in "fishing" for relevant artifacts from overwhelming sandbox reports.
- Users can now track threats of interest and receive updates about new detection opportunities.

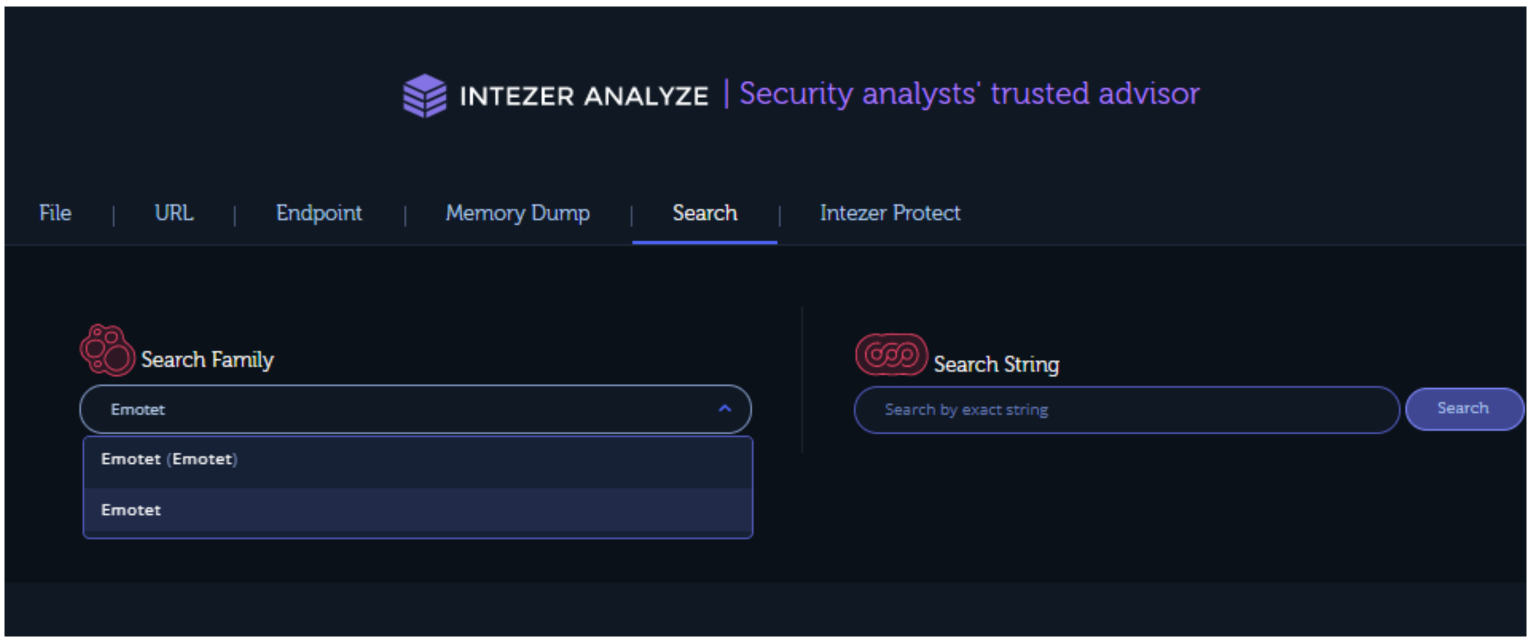
On Intezer's family page, you can find all the detection opportunities extracted per family. This capability, combined with our API, allows you to identify up-to-date behavioral artifacts to create rules to proactively hunt for the existence of a threat within your organization and create updated detection rules. You can "subscribe" to a threat family to ensure you do not miss the latest detection opportunities.

Tracking Threat Families in Practice

Intezer tracks thousands of threat actors and malware families that you can get updates on now.

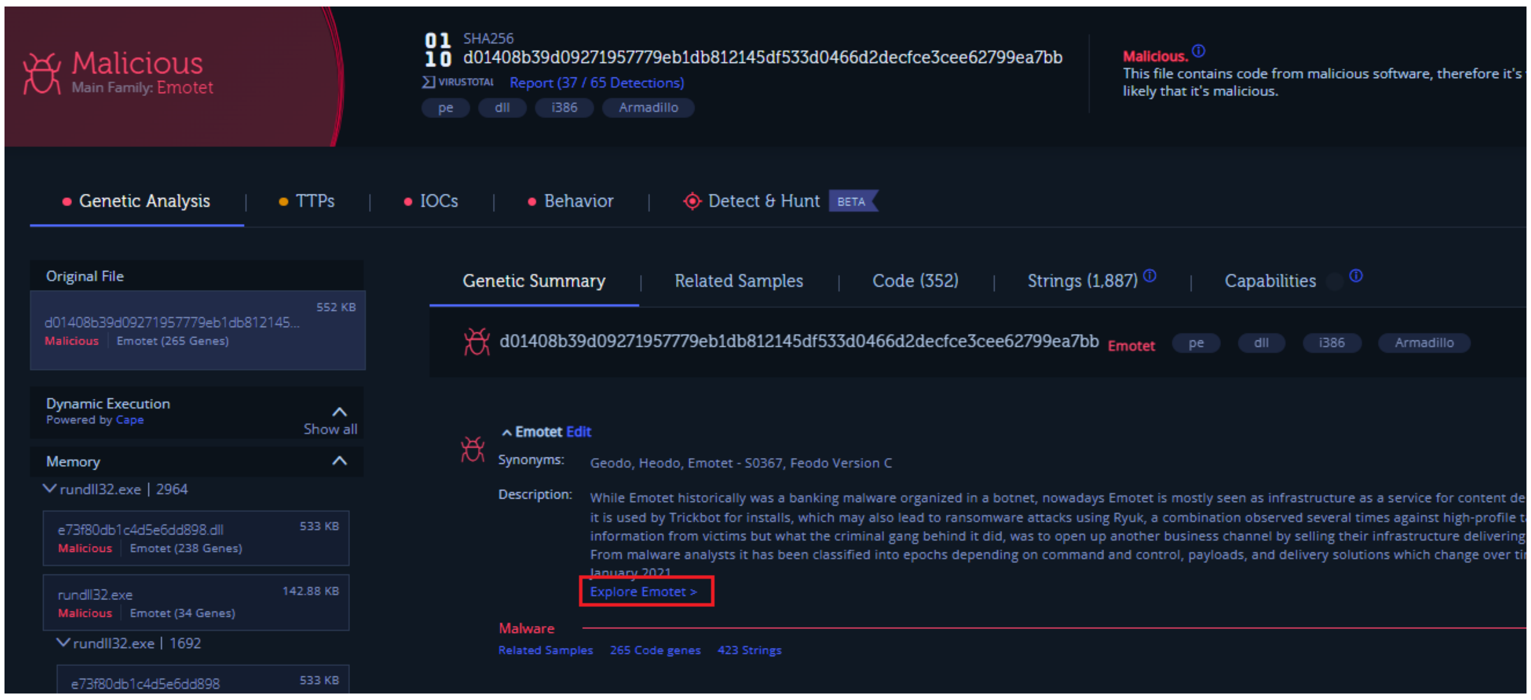
To get to the family page, search for a specific family or click on the family link from the analysis page. Let's browse to the Emotet family page.

From family search:



Using "Search" in Intezer to look up a threat actor or malware family.

From the analysis page:



SHA256
d01408b39d09271957779eb1db812145df533d0466d2decfce3cee62799ea7bb
VIRUSTOTAL Report (37 / 65 Detections)
pe dll i386 Armadillo

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

552 KB
d01408b39d09271957779eb1db812145...
Malicious | Emotet (265 Genes)

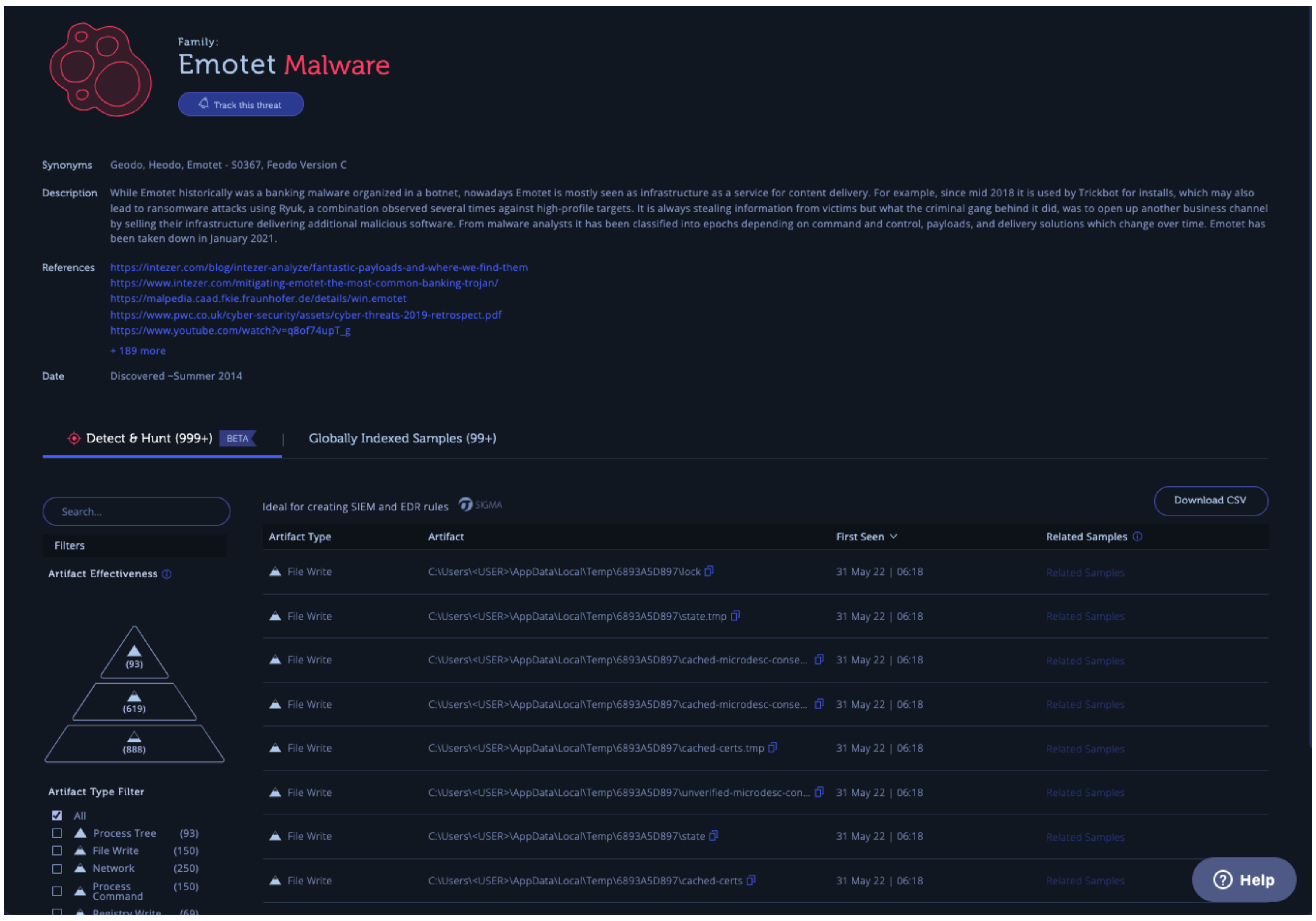
rundll32.exe | 2964
e73f80db1c4d5e6dd898.dll 533 KB
Malicious | Emotet (238 Genes)
rundll32.exe 142.88 KB
Malicious | Emotet (34 Genes)
rundll32.exe | 1692
e73f80db1c4d5e6dd898 533 KB

d01408b39d09271957779eb1db812145df533d0466d2decfce3cee62799ea7bb Emotet pe dll i386 Armadillo

Emotet Edit
Synonyms: Geodo, Heodo, Emotet - S0367, Feodo Version C
Description: While Emotet historically was a banking malware organized in a botnet, nowadays Emotet is mostly seen as infrastructure as a service for content de
it is used by Trickbot for installs, which may also lead to ransomware attacks using Ryuk, a combination observed several times against high-profile t
information from victims but what the criminal gang behind it did, was to open up another business channel by selling their infrastructure delivering
From malware analysts it has been classified into epochs depending on command and control, payloads, and delivery solutions which change over ti
January 2021

To see the Emotet family page, you'd click the "Explore Emotet" highlighted in red.

On the family page, you can find Detect & Hunt tab with the most updated detection opportunities for the family.



Family:

Emotet Malware

Synonyms Geodo, Heodo, Emotet - S0367, Feodo Version C

Description While Emotet historically was a banking malware organized in a botnet, nowadays Emotet is mostly seen as infrastructure as a service for content delivery. For example, since mid 2018 it is used by Trickbot for installs, which may also lead to ransomware attacks using Ryuk, a combination observed several times against high-profile targets. It is always stealing information from victims but what the criminal gang behind it did, was to open up another business channel by selling their infrastructure delivering additional malicious software. From malware analysts it has been classified into epochs depending on command and control, payloads, and delivery solutions which change over time. Emotet has been taken down in January 2021.

References https://intezer.com/blog/intezer-analyze/fantastic-payloads-and-where-we-find-them
https://www.intezer.com/mitigating-emotet-the-most-common-banking-trojan/
https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.youtube.com/watch?v=q8of74upT_g
+ 189 more

Date Discovered ~Summer 2014

Ideal for creating SIEM and EDR rules

Artifact Effectiveness

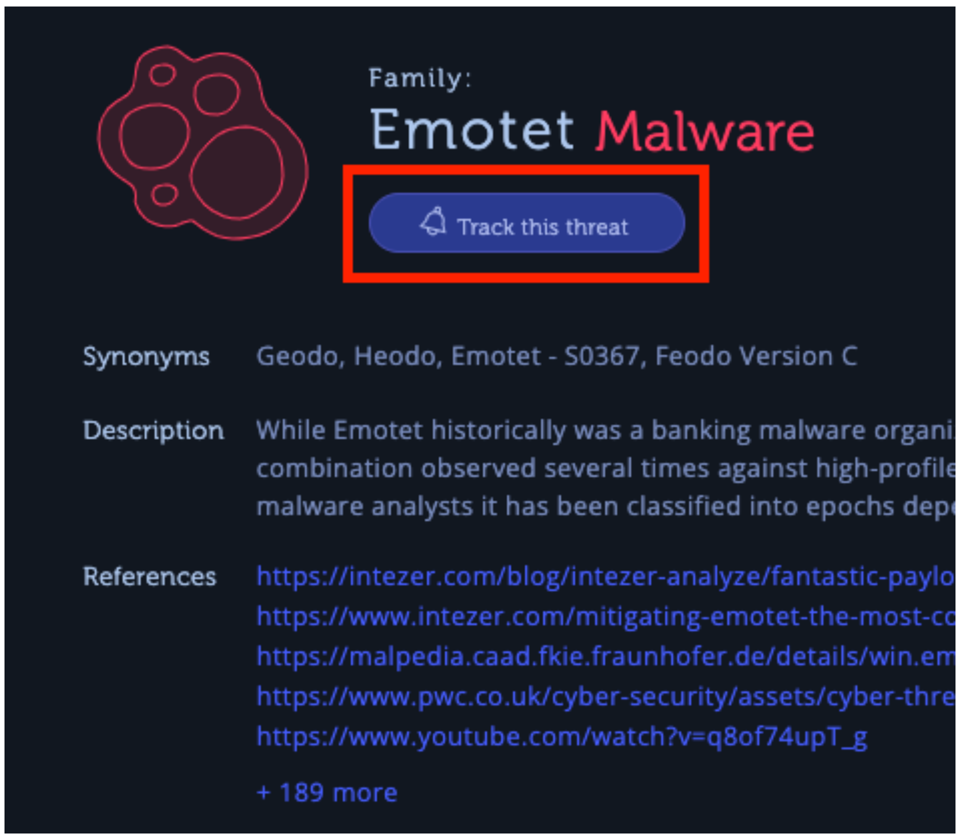
Artifact Type Filter

☑ All
☐ Process Tree (93)
☐ File Write (150)
☐ Network (250)
☐ Process Command (150)
☐ Registry Write (69)

Artifact Type	Artifact	First Seen	Related Samples
File Write	C:\Users\<USER>\AppData\Local\Temp\6893A5D897\lock	31 May 22 | 06:18	Related Samples
File Write	C:\Users\<USER>\AppData\Local\Temp\6893A5D897\state.tmp	31 May 22 | 06:18	Related Samples
File Write	C:\Users\<USER>\AppData\Local\Temp\6893A5D897\cached-microdesc-conse...	31 May 22 | 06:18	Related Samples
File Write	C:\Users\<USER>\AppData\Local\Temp\6893A5D897\cached-microdesc-conse...	31 May 22 | 06:18	Related Samples
File Write	C:\Users\<USER>\AppData\Local\Temp\6893A5D897\cached-certs.tmp	31 May 22 | 06:18	Related Samples
File Write	C:\Users\<USER>\AppData\Local\Temp\6893A5D897\unverified-microdesc-con...	31 May 22 | 06:18	Related Samples
File Write	C:\Users\<USER>\AppData\Local\Temp\6893A5D897\state	31 May 22 | 06:18	Related Samples
File Write	C:\Users\<USER>\AppData\Local\Temp\6893A5D897\cached-certs	31 May 22 | 06:18	Related Samples

Family page for the Emotet malware.

Track the threat to get updates and keep your detection content up-to-date.



Family:

Emotet Malware

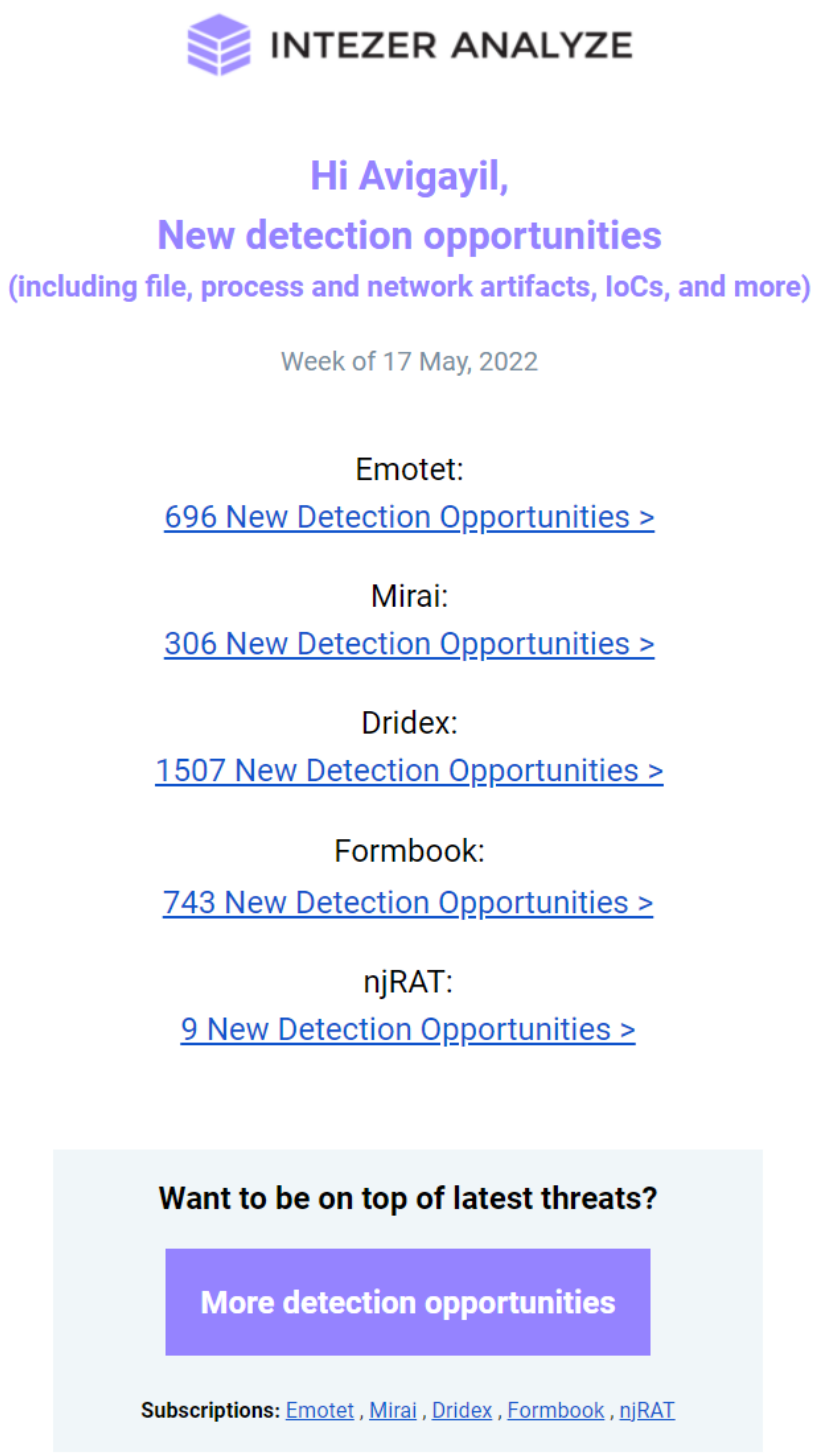
Synonyms Geodo, Heodo, Emotet - S0367, Feodo Version C

Description While Emotet historically was a banking malware organi
combination observed several times against high-profile
malware analysts it has been classified into epochs depe

References https://intezer.com/blog/intezer-analyze/fantastic-paylo
https://www.intezer.com/mitigating-emotet-the-most-co
https://malpedia.caad.fkie.fraunhofer.de/details/win.em
https://www.pwc.co.uk/cyber-security/assets/cyber-thre
https://www.youtube.com/watch?v=q8of74upT_g
+ 189 more

Tracking a threat now signs you up for regular updates when Intezer discovers new detection opportunities.

You will receive a weekly email notifying you about any new detection opportunities for threats you have subscribed to.



INTEZER ANALYZE

Hi Avigayil,

New detection opportunities

(including file, process and network artifacts, IoCs, and more)

Week of 17 May, 2022

Emotet:

696 New Detection Opportunities >

Mirai:

306 New Detection Opportunities >

Dridex:

1507 New Detection Opportunities >

Formbook:

743 New Detection Opportunities >

njRAT:

9 New Detection Opportunities >

Want to be on top of latest threats?

More detection opportunities

Subscriptions: Emotet , Mirai , Dridex , Formbook , njRAT

Creating Rules and Searches from Detection Opportunities

To accelerate the process of proactive and reactive threat hunting, you should make sure that you use high-quality detections and that you use automation where applicable. The detection opportunities Intezer provides are actionable and can be filtered based on an effectiveness pyramid that takes inspiration from the Pyramid of Pain. All data is available via API to build automation around it.

To learn how to convert detection opportunities to rules, check out our SOC Level Up series that covers techniques and knowledge for improving SOC skills.

Detect & Hunt and family tracking are available now for Intezer's enterprise customers. Reach us to book 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.

detection engineering detection opportunities detection rules Incident Response IoCs pyramid of pain Threat Detection