Threatray – Getting started

Session 2 – Intelligence capabilities

THREATRAY

Content

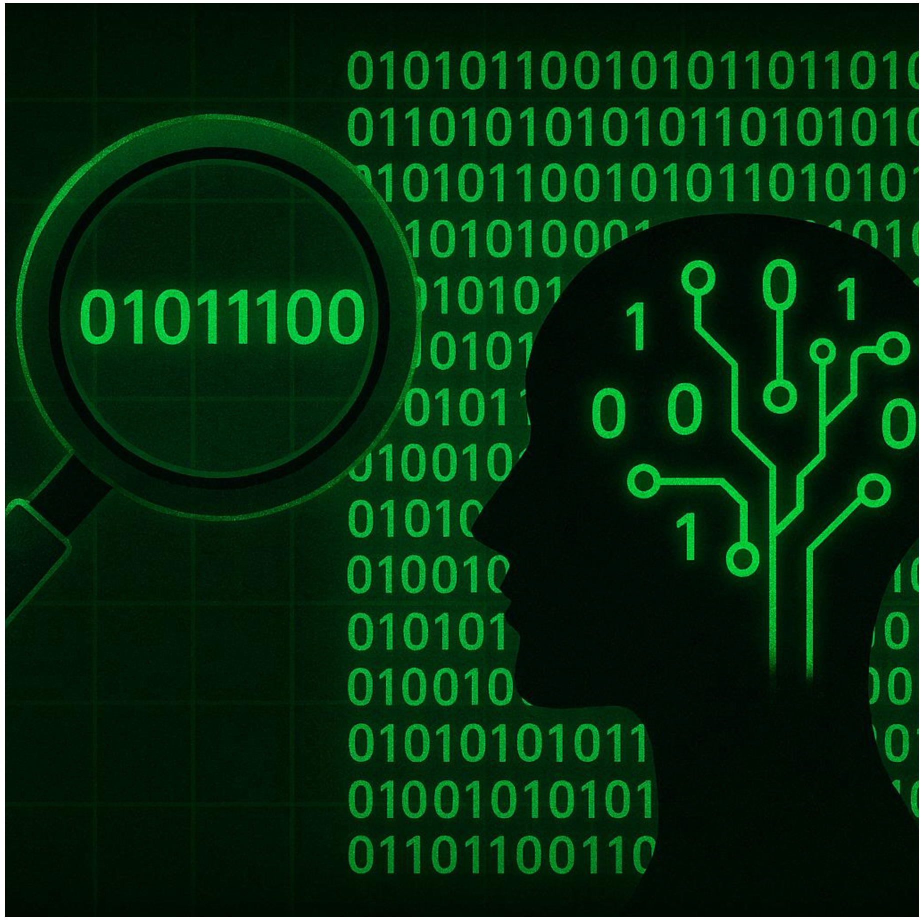
- Background information on our intelligence capabilities
- Classical search, finding IOCs fast
- Code search (finding OSINT through code and retro-hunting for code)
- Code intelligence

Intro

Threatray intelligence capabilities

- Threatray not only has deep malware analysis capabilities to analyse a malware “in isolation” but also **unique capabilities in malware intelligence.**

- Intelligence analysis in Threatray has two aspects **intelligence aided investigations** of new malware, as well as **intelligence production**.



Threatray intelligence capabilities

- Intelligence analysis is **malware data and search** driven.
- For the data side, the Threatray platform contains a **public and private malware repository.**

  The public repository is shared by all Threatray users and contains malware curated by Threatray:

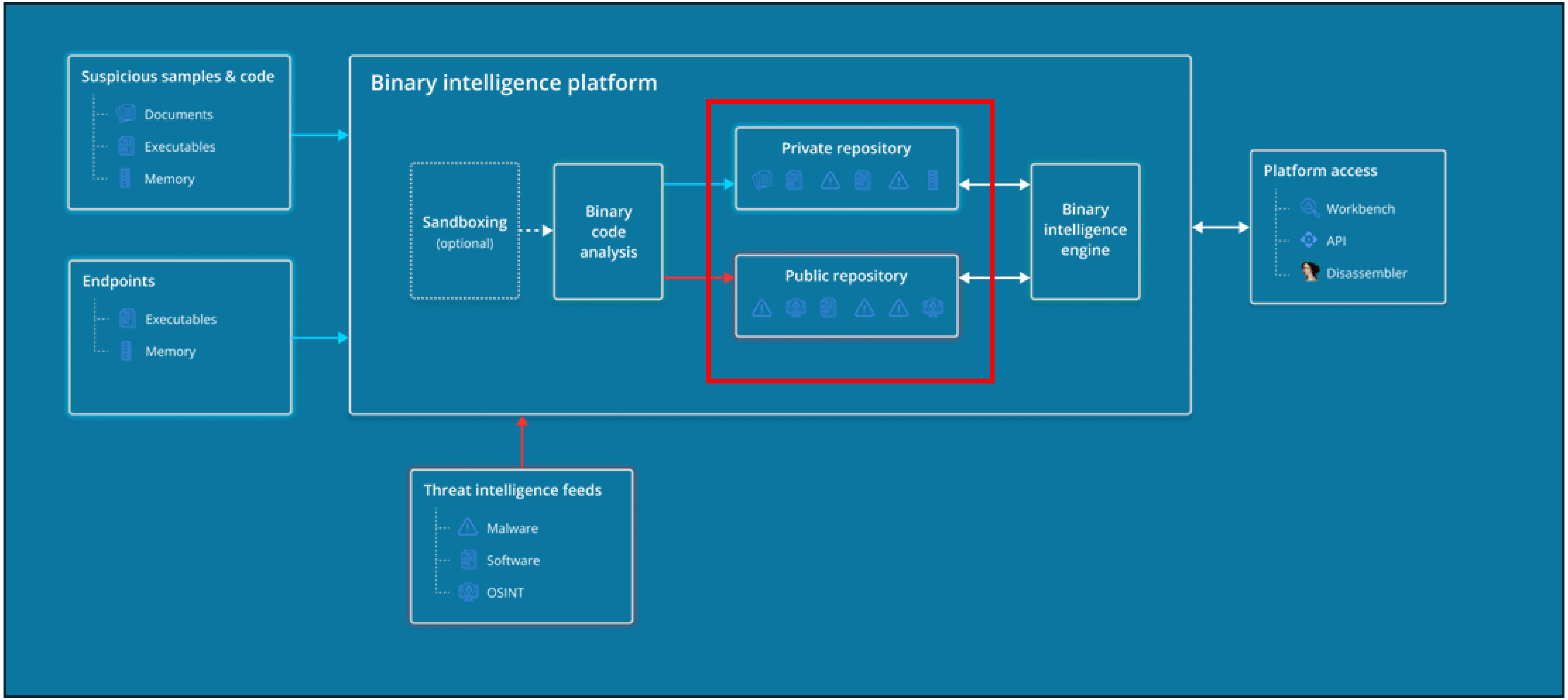
  - Malware samples from partners, from harvesting OSINT sample,….
  - NOT from our users!
  - Contains cybercrime, APTs, C2s etc.

- For many of **our users the private repository also serves as a malware repository** for their own malware, making it analysable and **turning their own malware collection into intelligence.**

  New Threatray users, can **import their existing malware collection into Threatray.**

- **For the search side of things,** we provide
  - **classical search** (e.g.,. for IPs, domains, process names, mutexes,…) and
  - **unique code search capabilities** that allow you to find code-wise similar samples to the one under investigation.

Threatray architecture – Two Data Repositories



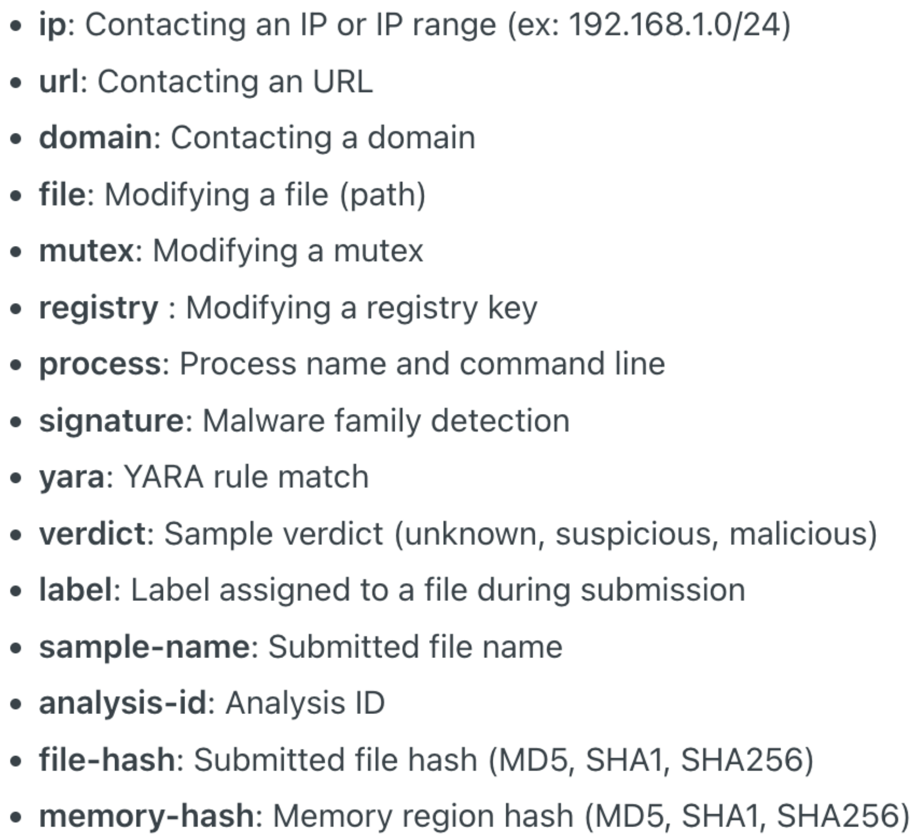
Classical search capabilities

Classical search

- Classical search is like what you know from existing malware platforms, with the **important difference, that you can search our public repository *and* your private repository (”we make your private analyses searchable”)**

- **Search across public and private is seamless,** so that you can relate what your own malware to malware seen globally and vice versa.

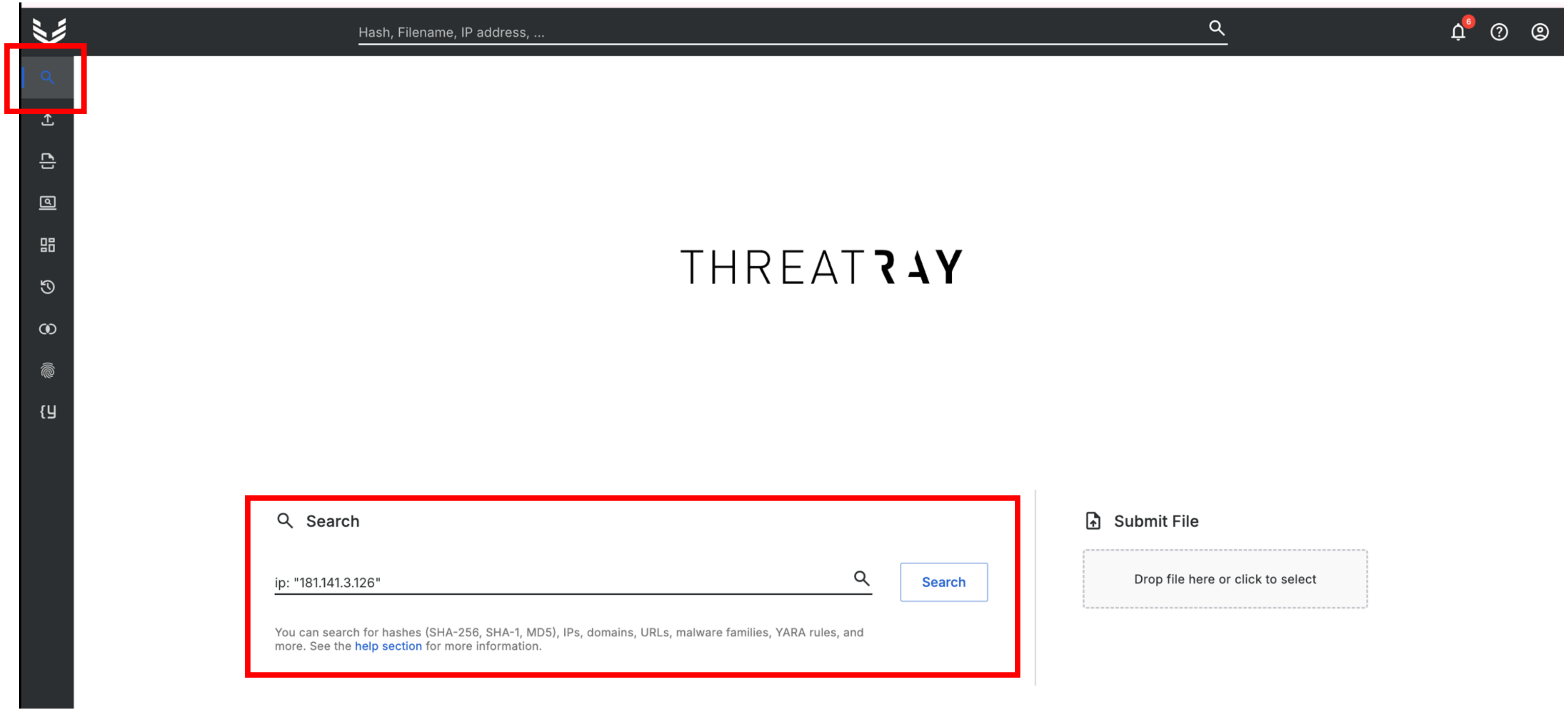
- **What is unique in Threatray is the statistics view over the search results, allowing to identify cluster properties and IOCs (see later)**



- **ip**: Contacting an IP or IP range (ex: 192.168.1.0/24)
- **url**: Contacting an URL
- **domain**: Contacting a domain
- **file**: Modifying a file (path)
- **mutex**: Modifying a mutex
- **registry** : Modifying a registry key
- **process**: Process name and command line
- **signature**: Malware family detection
- **yara**: YARA rule match
- **verdict**: Sample verdict (unknown, suspicious, malicious)
- **label**: Label assigned to a file during submission
- **sample-name**: Submitted file name
- **analysis-id**: Analysis ID
- **file-hash**: Submitted file hash (MD5, SHA1, SHA256)
- **memory-hash**: Memory region hash (MD5, SHA1, SHA256)

Entities we can search for

Where can you launch a search?



Hash, Filename, IP address, ...
THREATRAY
Submit File
Drop file here or click to select

Search

ip: "181.141.3.126"

Search

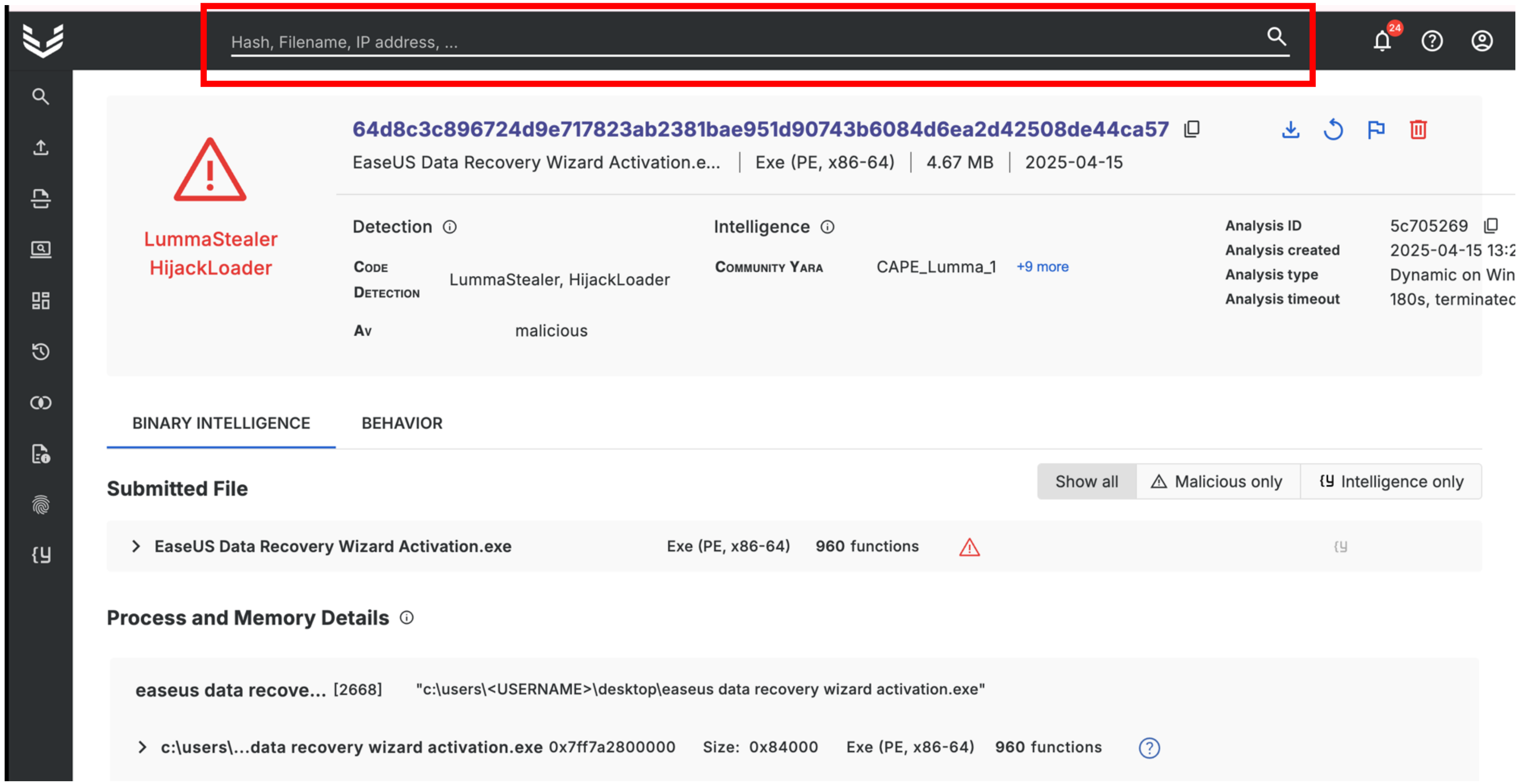
You can search for hashes (SHA-256, SHA-1, MD5), IPs, domains, URLs, malware families, YARA rules, and more. See the help section for more information.

(1) Search view

(2) Enter query here

Where can you launch a search?

There is a search bar on top of any analysis to quickly launch searches



Hash, Filename, IP address, ...

64d8c3c896724d9e717823ab2381bae951d90743b6084d6ea2d42508de44ca57

EaseUS Data Recovery Wizard Activation.e... | Exe (PE, x86-64) | 4.67 MB | 2025-04-15

LummaStealer
HijackLoader

Detection

Code Detection: LummaStealer, HijackLoader

Av: malicious

Intelligence

Community Yara: CAPE_Lumma_1 +9 more

Analysis ID	5c705269
Analysis created	2025-04-15 13:2
Analysis type	Dynamic on Win
Analysis timeout	180s, terminatec

Submitted File

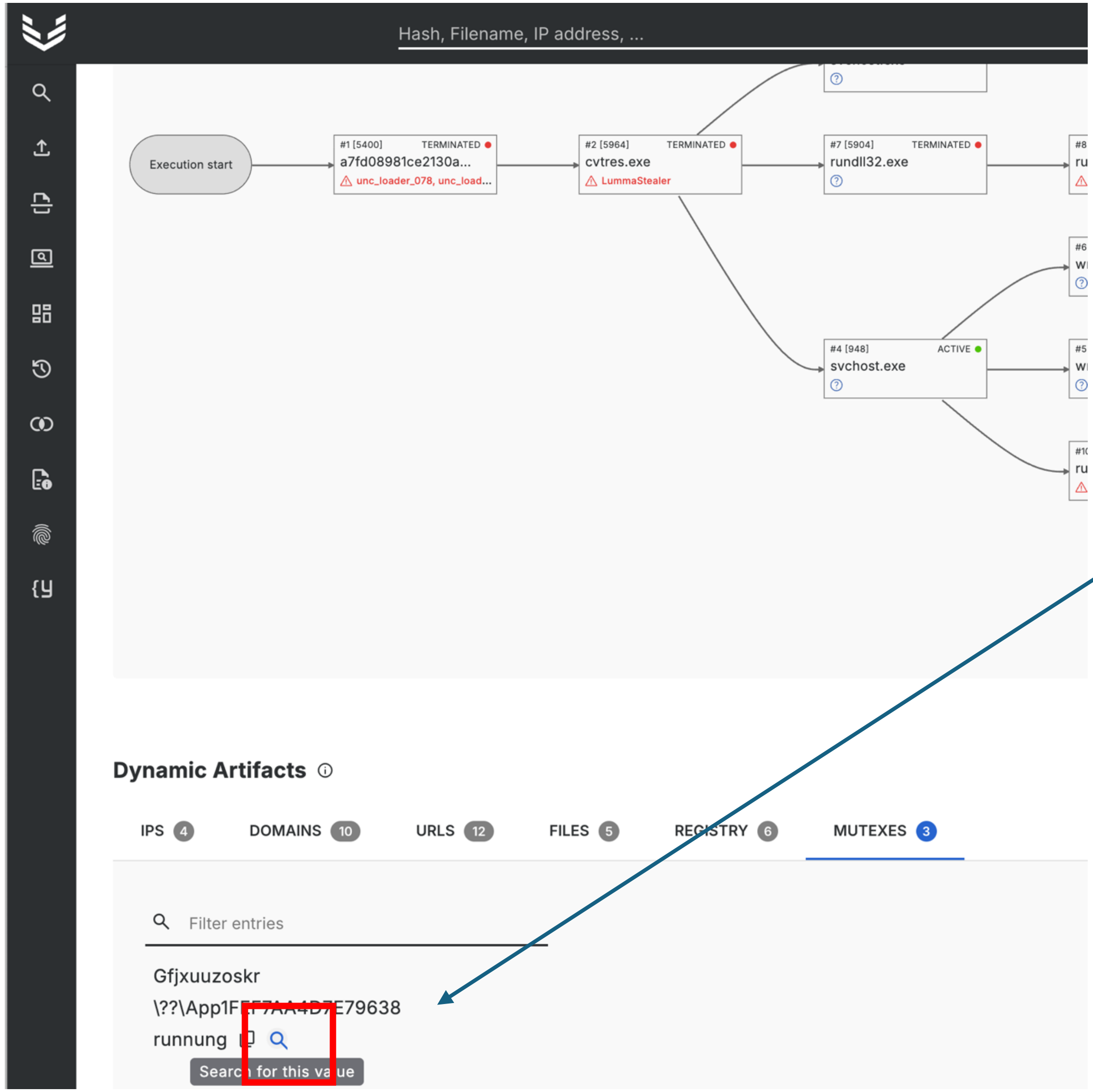
EaseUS Data Recovery Wizard Activation.exe   Exe (PE, x86-64)   960 functions

Process and Memory Details

easeus data recove... [2668]   "c:\users\<USERNAME>\desktop\easeus data recovery wizard activation.exe"

c:\users\...data recovery wizard activation.exe 0x7ff7a2800000   Size: 0x84000   Exe (PE, x86-64)   960 functions

Where can you launch a search?



Dynamic Artifacts

IPS 4 DOMAINS 10 URLS 12 FILES 5 REGISTRY 6 MUTEXES 3

Filter entries

Gfjxuuzoskr
\??\App1FEF7AA4D7E79638
runnung

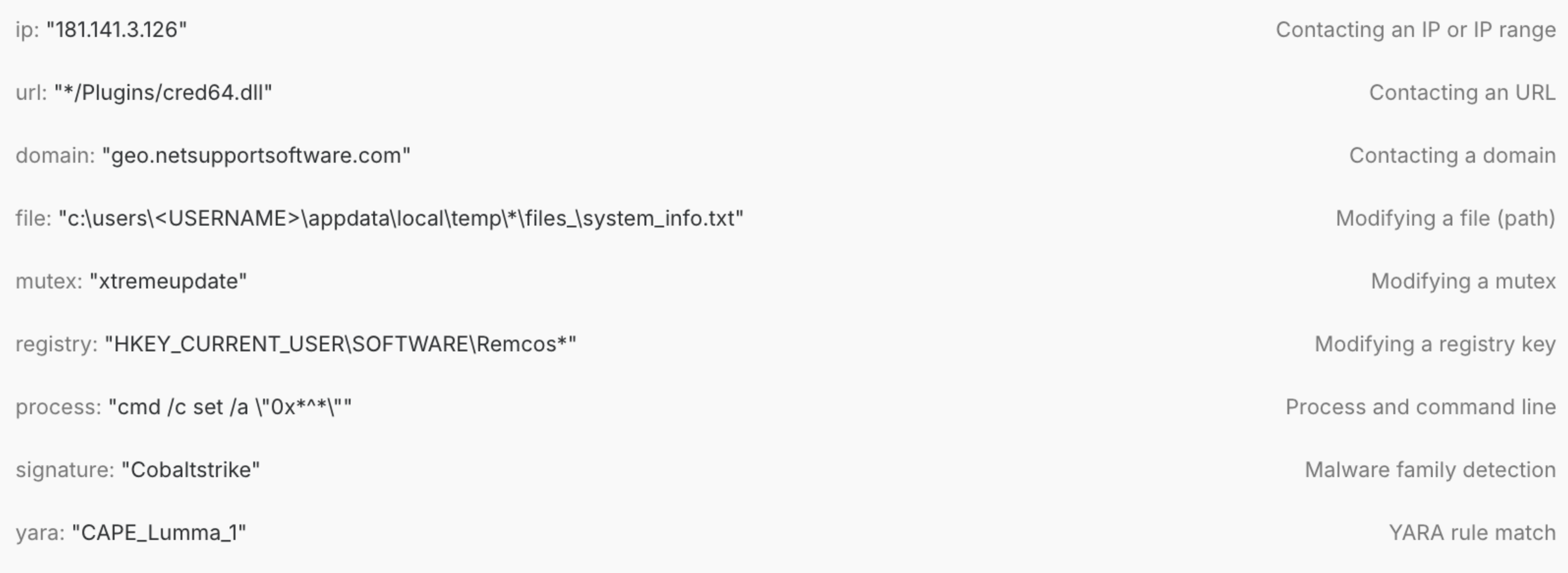
Search for this value

In the behavior report, there is a search icon next to each dynamic artifact.

THREATRAY

Search syntax

We support autocompletion, and wildcards “*”, for AND you can simply use multiple queries in the same search bar, no OR at the moment.



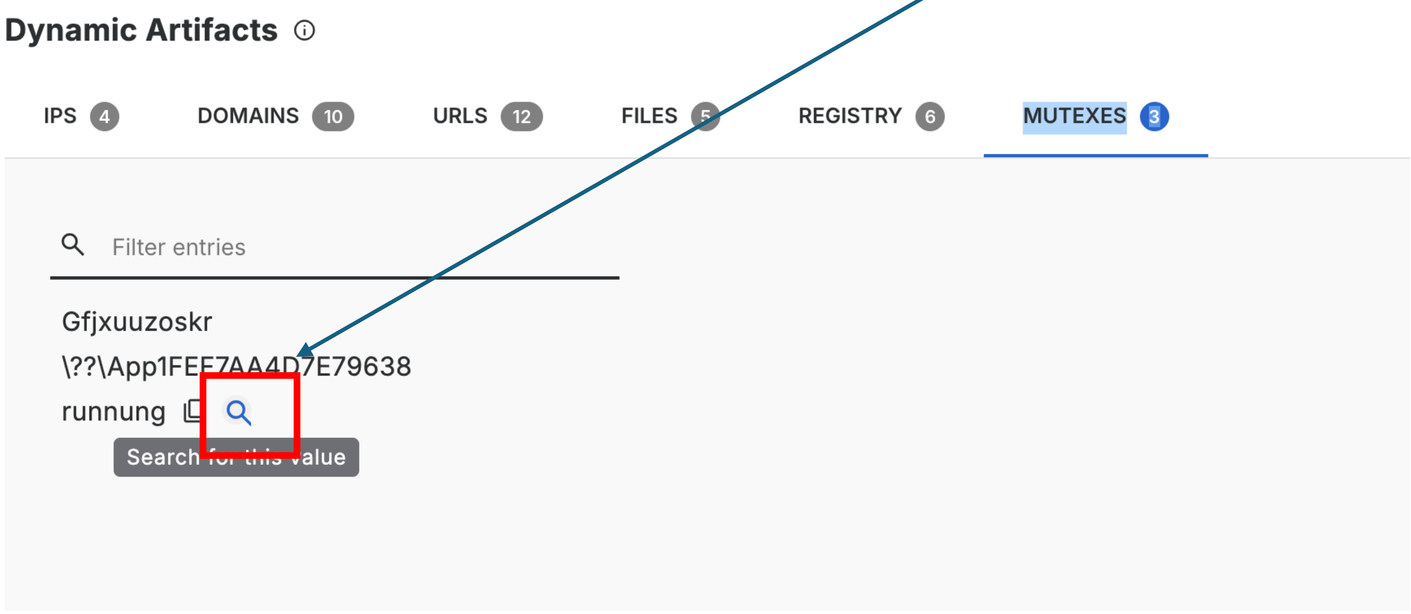
ip: "181.141.3.126"	Contacting an IP or IP range
url: "*/Plugins/cred64.dll"	Contacting an URL
domain: "geo.netsupportsoftware.com"	Contacting a domain
file: "c:\users\<USERNAME>\appdata\local\temp\*\files_\system_info.txt"	Modifying a file (path)
mutex: "xtremeupdate"	Modifying a mutex
registry: "HKEY_CURRENT_USER\SOFTWARE\Remcos*"	Modifying a registry key
process: "cmd /c set /a \"0x*^*\""	Process and command line
signature: "Cobaltstrike"	Malware family detection
yara: "CAPE_Lumma_1"	YARA rule match

See here https://docs.threatray.com/docs/search

Search example – Finding IOC

- **In this worked examples we show how we can use search to identify a mutex type IOC for the Latrodectus malware family.**

- We are investigating the dynamic artifacts in the analysis view and click on the “running” mutex to search for it.



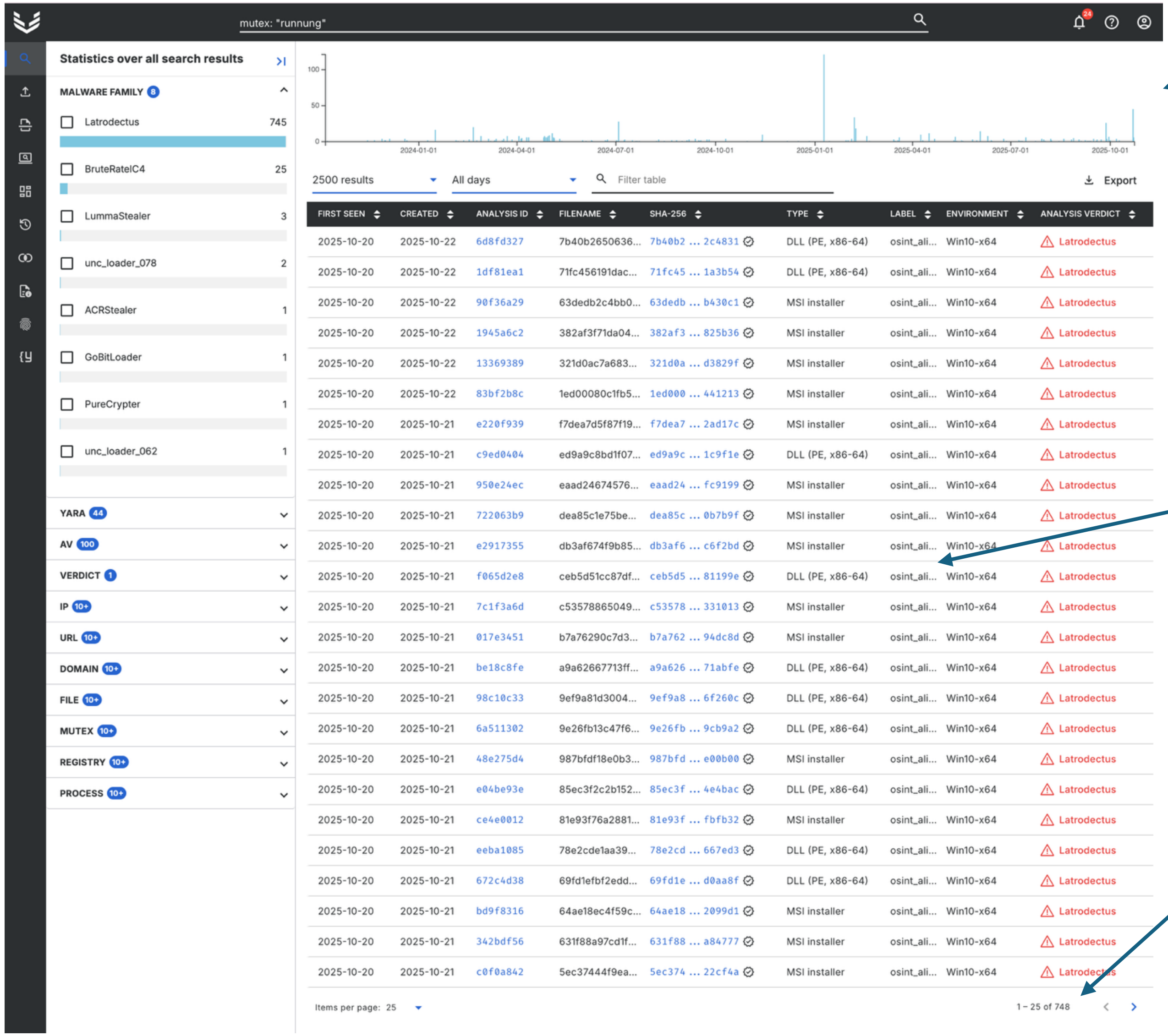
Gfjxuuzoskr
\??\App1FEE7AA4D7E79638
runnung

Search example – Finding IOC

Distribution of first seen dates of samples

Static results over the search result set.

Think of it as “cluster statistics”



mutex: "runnung"

Statistics over all search results

MALWARE FAMILY 8

□ Latrodectus	745
□ BruteRatelC4	25
□ LummaStealer	3
□ unc_loader_078	2
□ ACRStealer	1
□ GoBitLoader	1
□ PureCrypter	1
□ unc_loader_062	1

YARA 44

AV 100

VERDICT 1

IP 10+

URL 10+

DOMAIN 10+

FILE 10+

MUTEX 10+

REGISTRY 10+

PROCESS 10+

2500 results · All days · Filter table · Export

FIRST SEEN	CREATED	ANALYSIS ID	FILENAME	SHA-256	TYPE	LABEL	ENVIRONMENT	ANALYSIS VERDICT
2025-10-20	2025-10-22	6d8fd327	7b40b2650636...	7b40b2 ... 2c4831	DLL (PE, x86-64)	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-22	1df81ea1	71fc456191dac...	71fc45 ... 1a3b54	DLL (PE, x86-64)	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-22	90f36a29	63dedb2c4bb0...	63dedb ... b430c1	MSI installer	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-22	1945a6c2	382af3f71da04...	382af3 ... 825b36	MSI installer	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-22	13369389	321d0ac7a683...	321d0a ... d3829f	MSI installer	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-22	83bf2b8c	1ed00080c1fb5...	1ed000 ... 441213	MSI installer	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	e220f939	f7dea7d5f87f19...	f7dea7 ... 2ad17c	MSI installer	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	c9ed0404	ed9a9c8bd1f07...	ed9a9c ... 1c9f1e	DLL (PE, x86-64)	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	950e24ec	eaad24674576...	eaad24 ... fc9199	MSI installer	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	722063b9	dea85c1e75be...	dea85c ... 0b7b9f	MSI installer	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	e2917355	db3af674f9b85...	db3af6 ... c6f2bd	MSI installer	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	f065d2e8	ceb5d51cc87df...	ceb5d5 ... 81199e	DLL (PE, x86-64)	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	7c1f3a6d	c53578865049...	c53578 ... 331013	MSI installer	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	017e3451	b7a76290c7d3...	b7a762 ... 94dc8d	MSI installer	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	be18c8fe	a9a62667713ff...	a9a626 ... 71abfe	DLL (PE, x86-64)	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	98c10c33	9ef9a81d3004...	9ef9a8 ... 6f260c	DLL (PE, x86-64)	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	6a511302	9e26fb13c47f6...	9e26fb ... 9cb9a2	DLL (PE, x86-64)	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	48e275d4	987bfdf18e0b3...	987bfd ... e00b00	MSI installer	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	e04be93e	85ec3f2c2b152...	85ec3f ... 4e4bac	DLL (PE, x86-64)	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	ce4e0012	81e93f76a2881...	81e93f ... fbfb32	MSI installer	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	eeba1085	78e2cde1aa39...	78e2cd ... 667ed3	DLL (PE, x86-64)	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	672c4d38	69fd1efbf2edd...	69fd1e ... d0aa8f	DLL (PE, x86-64)	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	bd9f8316	64ae18ec4f59c...	64ae18 ... 2099d1	MSI installer	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	342bdf56	631f88a97cd1f...	631f88 ... a84777	MSI installer	osint_ali...	Win10-x64	Latrodectus
2025-10-20	2025-10-21	c0f0a842	5ec37444f9ea...	5ec374 ... 22cf4a	MSI installer	osint_ali...	Win10-x64	Latrodectus

Items per page: 25

1 – 25 of 748

Matching samples / analyses.

Pivot to any of them

Total analyses found (748)

THREATRAY

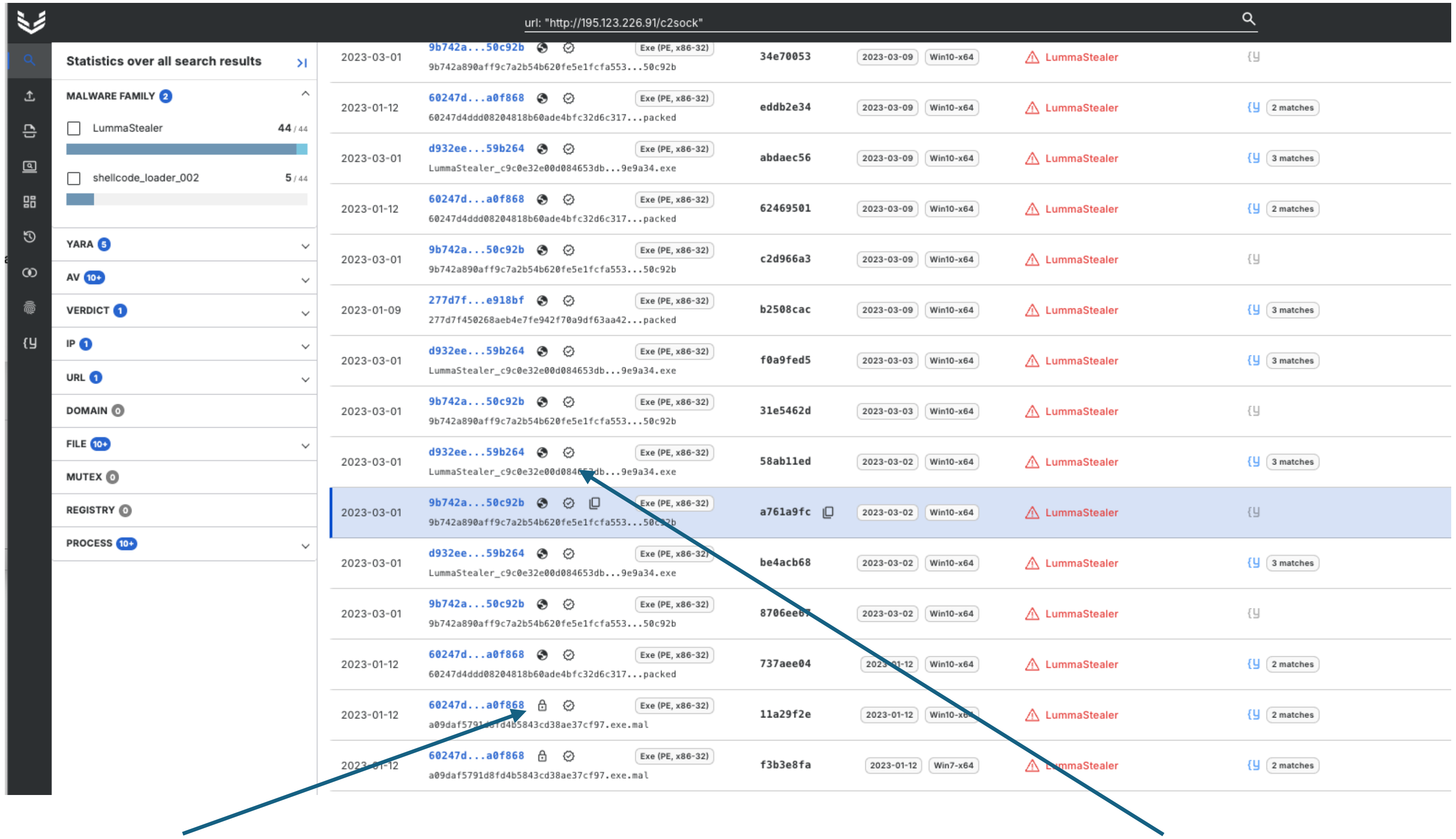
Search example – Finding IOC

The “cluster statistics” for the ”runnung mutex” show the following (see previous slide):

- We have found 839 files with that mutex
- Of those 836 files 839 are classified as Latrodectus

→ The mutex “runnung” and the “Latrodectus” family are strongly correlated, and thus very likely the “runnung” mutex is a good IOC for the family.

Private , global, samples from OSINT



url: "http://195.123.226.91/c2sock"

Statistics over all search results

MALWARE FAMILY 2

- ☐ LummaStealer 44 / 44
- ☐ shellcode_loader_002 5 / 44

YARA 5

AV 10+

VERDICT 1

IP 1

URL 1

DOMAIN 0

FILE 10+

MUTEX 0

REGISTRY 0

PROCESS 10+

2023-03-01	9b742a...50c92b 9b742a890aff9c7a2b54b620fe5e1fcfa553...50c92b	🌐	Exe (PE, x86-32)	34e70053	2023-03-09	Win10-x64	LummaStealer	
2023-01-12	60247d...a0f868 60247d4ddd08204818b60ade4bfc32d6c317...packed	🌐	Exe (PE, x86-32)	eddb2e34	2023-03-09	Win10-x64	LummaStealer	2 matches
2023-03-01	d932ee...59b264 LummaStealer_c9c0e32e00d084653db...9e9a34.exe	🌐	Exe (PE, x86-32)	abdaec56	2023-03-09	Win10-x64	LummaStealer	3 matches
2023-01-12	60247d...a0f868 60247d4ddd08204818b60ade4bfc32d6c317...packed	🌐	Exe (PE, x86-32)	62469501	2023-03-09	Win10-x64	LummaStealer	2 matches
2023-03-01	9b742a...50c92b 9b742a890aff9c7a2b54b620fe5e1fcfa553...50c92b	🌐	Exe (PE, x86-32)	c2d966a3	2023-03-09	Win10-x64	LummaStealer	
2023-01-09	277d7f...e918bf 277d7f450268aeb4e7fe942f70a9df63aa42...packed	🌐	Exe (PE, x86-32)	b2508cac	2023-03-09	Win10-x64	LummaStealer	3 matches
2023-03-01	d932ee...59b264 LummaStealer_c9c0e32e00d084653db...9e9a34.exe	🌐	Exe (PE, x86-32)	f0a9fed5	2023-03-03	Win10-x64	LummaStealer	3 matches
2023-03-01	9b742a...50c92b 9b742a890aff9c7a2b54b620fe5e1fcfa553...50c92b	🌐	Exe (PE, x86-32)	31e5462d	2023-03-03	Win10-x64	LummaStealer	
2023-03-01	d932ee...59b264 LummaStealer_c9c0e32e00d084653db...9e9a34.exe	🌐	Exe (PE, x86-32)	58ab11ed	2023-03-02	Win10-x64	LummaStealer	3 matches
2023-03-01	9b742a...50c92b 9b742a890aff9c7a2b54b620fe5e1fcfa553...50c92b	🌐	Exe (PE, x86-32)	a761a9fc	2023-03-02	Win10-x64	LummaStealer	
2023-03-01	d932ee...59b264 LummaStealer_c9c0e32e00d084653db...9e9a34.exe	🌐	Exe (PE, x86-32)	be4acb68	2023-03-02	Win10-x64	LummaStealer	3 matches
2023-03-01	9b742a...50c92b 9b742a890aff9c7a2b54b620fe5e1fcfa553...50c92b	🌐	Exe (PE, x86-32)	8706ee67	2023-03-02	Win10-x64	LummaStealer	
2023-01-12	60247d...a0f868 60247d4ddd08204818b60ade4bfc32d6c317...packed	🌐	Exe (PE, x86-32)	737aee04	2023-01-12	Win10-x64	LummaStealer	2 matches
2023-01-12	60247d...a0f868 a09daf5791d8fd4b5843cd38ae37cf97.exe.mal	🔒	Exe (PE, x86-32)	11a29f2e	2023-01-12	Win10-x64	LummaStealer	2 matches
2023-01-12	60247d...a0f868 a09daf5791d8fd4b5843cd38ae37cf97.exe.mal	🔒	Exe (PE, x86-32)	f3b3e8fa	2023-01-12	Win7-x64	LummaStealer	2 matches

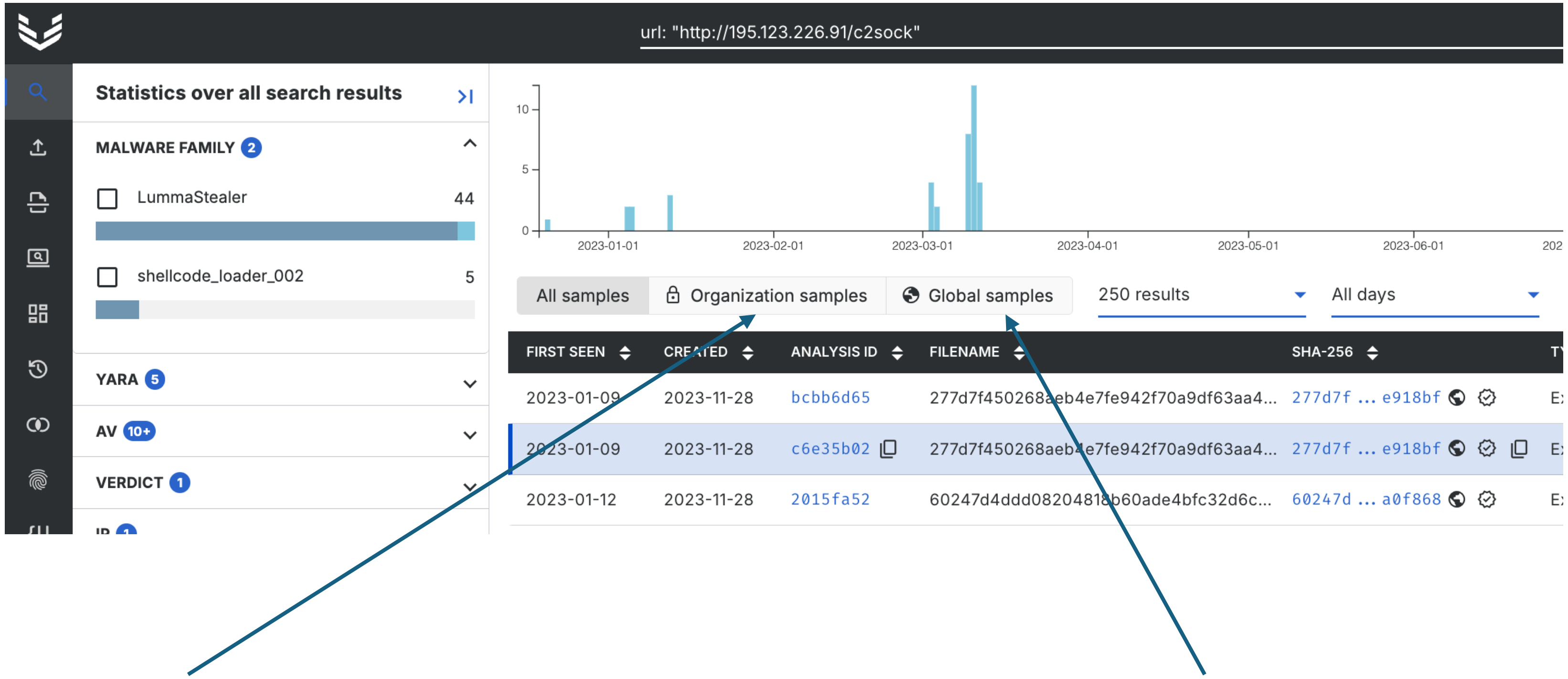
Private organization samples

🔒

Global samples

🌐

Filtering for private and global samples



url: "http://195.123.226.91/c2sock"

FIRST SEEN	CREATED	ANALYSIS ID	FILENAME	SHA-256	T
2023-01-09	2023-11-28	bcbb6d65	277d7f450268aeb4e7fe942f70a9df63aa4...	277d7f ... e918bf	E:
2023-01-09	2023-11-28	c6e35b02	277d7f450268aeb4e7fe942f70a9df63aa4...	277d7f ... e918bf	E:
2023-01-12	2023-11-28	2015fa52	60247d4ddd08204818b60ade4bfc32d6c...	60247d ... a0f868	E:

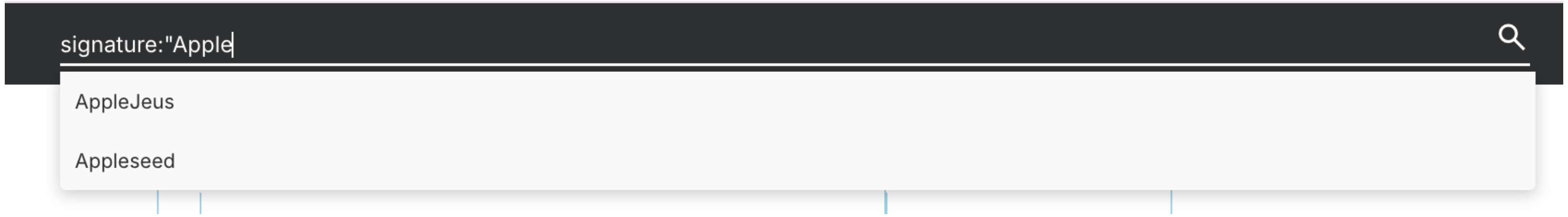
Private organization samples

Global samples

Searching for malware families

- When investigating malware families, a searches by family name can be tremendously useful.

  For family name searches we have auto completion, use the “signature:” search operator:



```
signature:"Apple
```

AppleJeus

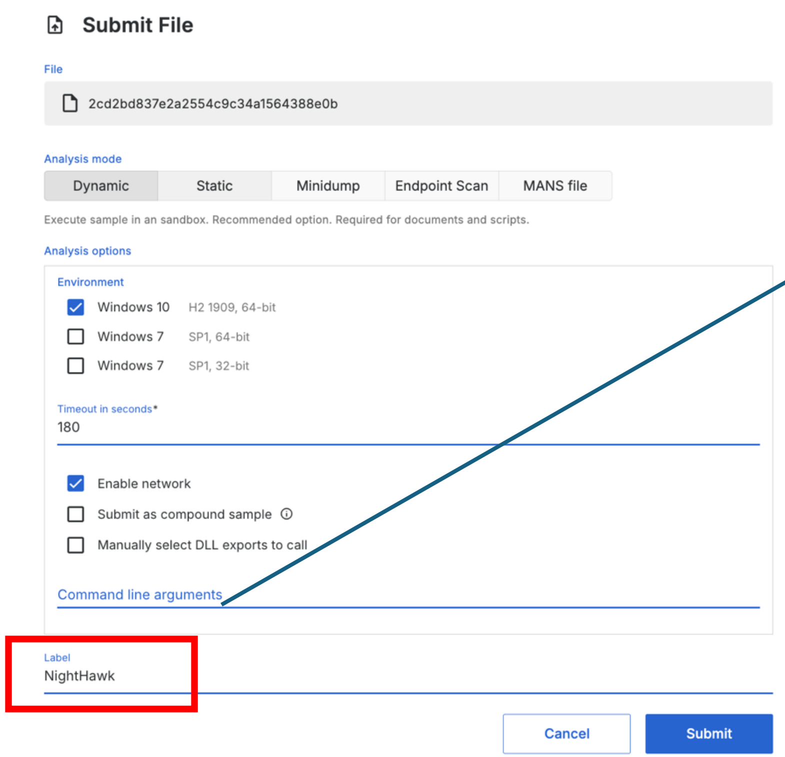
Appleseed

- You can also search by YARA rules names:

  ```
  yara:"win_brute_ratel_c4_a0"
  ```

- **Note:** The “signature:” search covers all samples, whereas “yara:” search only covers samples that were ingested after a YARA rule became active.

Search by label



Submit File

File

2cd2bd837e2a2554c9c34a1564388e0b

Analysis mode

Execute sample in an sandbox. Recommended option. Required for documents and scripts.

Analysis options

Environment

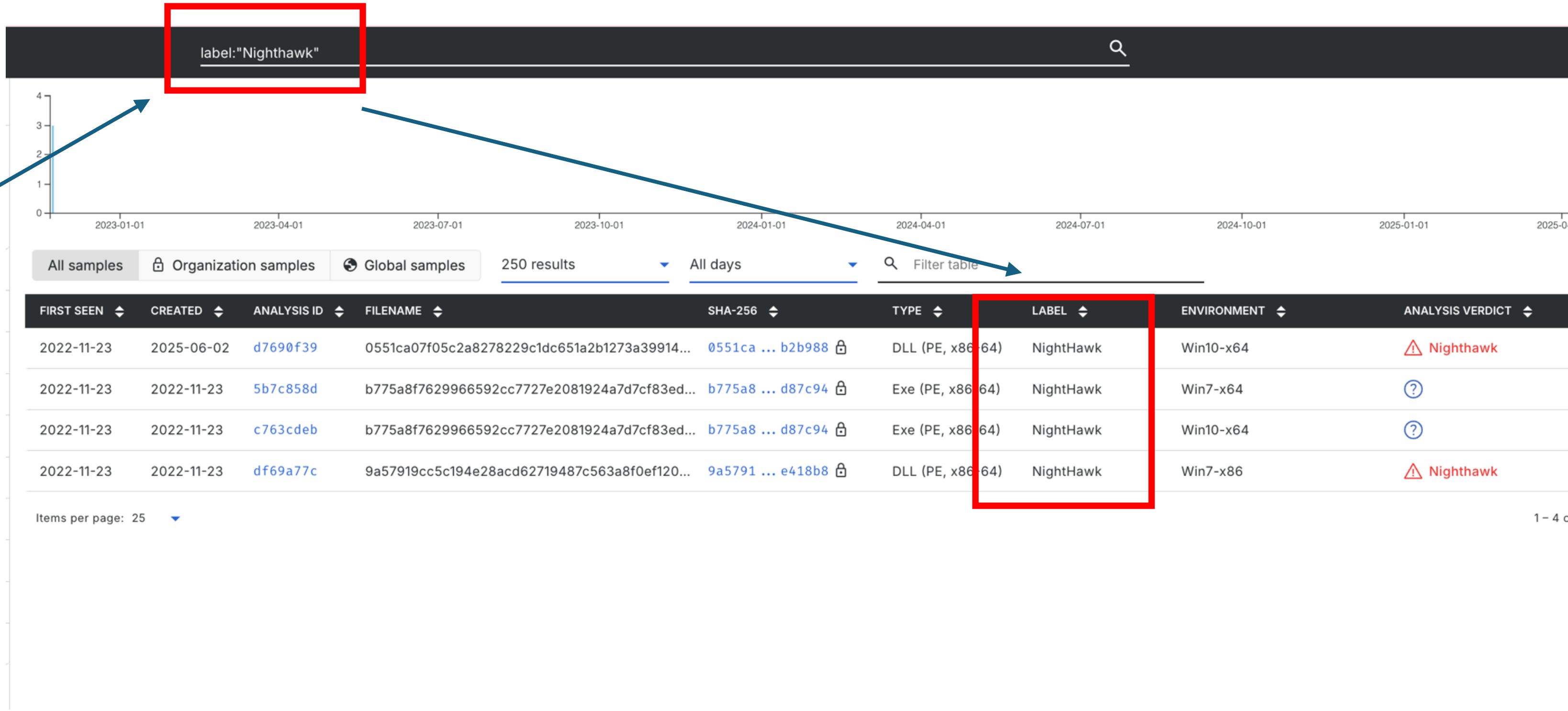
☑ Windows 10 H2 1909, 64-bit
□ Windows 7 SP1, 64-bit
□ Windows 7 SP1, 32-bit

Timeout in seconds*
180

☑ Enable network
□ Submit as compound sample ⓘ
□ Manually select DLL exports to call

Command line arguments

Label
NightHawk



label:"Nighthawk"

FIRST SEEN	CREATED	ANALYSIS ID	FILENAME	SHA-256	TYPE	LABEL	ENVIRONMENT	ANALYSIS VERDICT
2022-11-23	2025-06-02	d7690f39	0551ca07f05c2a8278229c1dc651a2b1273a39914...	0551ca ... b2b988	DLL (PE, x86-64)	NightHawk	Win10-x64	⚠ Nighthawk
2022-11-23	2022-11-23	5b7c858d	b775a8f7629966592cc7727e2081924a7d7cf83ed...	b775a8 ... d87c94	Exe (PE, x86-64)	NightHawk	Win7-x64	?
2022-11-23	2022-11-23	c763cdeb	b775a8f7629966592cc7727e2081924a7d7cf83ed...	b775a8 ... d87c94	Exe (PE, x86-64)	NightHawk	Win10-x64	?
2022-11-23	2022-11-23	df69a77c	9a57919cc5c194e28acd62719487c563a8f0ef120...	9a5791 ... e418b8	DLL (PE, x86-64)	NightHawk	Win7-x86	⚠ Nighthawk

Items per page: 25

1 – 4

Search & find samples by using the label that was given upon samples submission

Code search

OSINT search

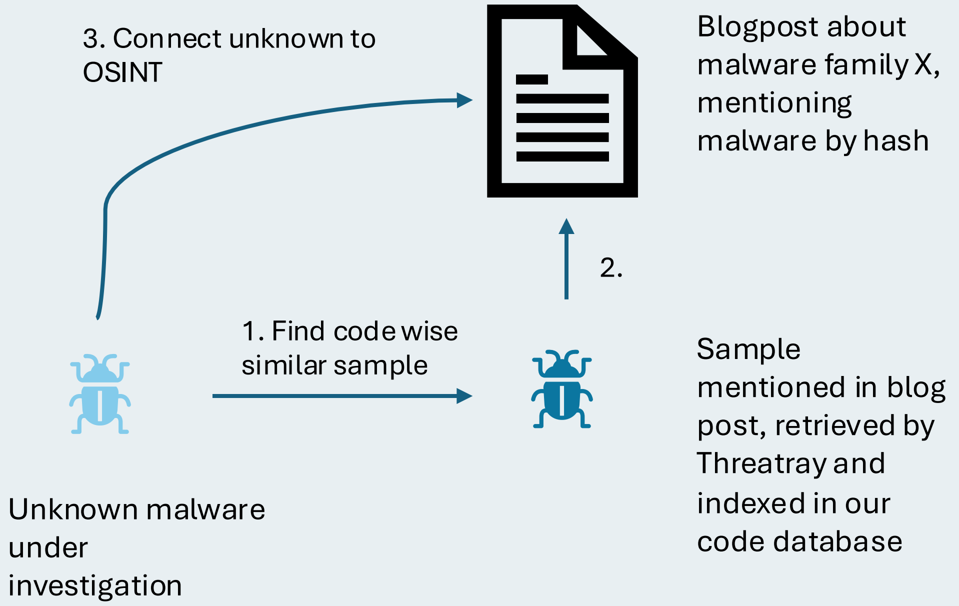
- **What is OSINT search?** The feature finds OSINT reports, like blogs, research articles, Tweets, that mention malware samples which are code-wise similar to the code region under investigation. In short: it finds relevant OSINT through code similarity. This capability significantly enhances our ability to discover relevant OSINT and accelerates investigation processes.

- **Discover OSINT in a Whole New Way.** This is a completely new and unique approach to searching for OSINT reports.

- **Why is it useful?**
  - **Uncover hidden insights:** Find OSINT you wouldn't discover through traditional search methods.
  - **Get highly relevant results:** Identify OSINT directly related to the code you're investigating — often far more precise, as it's based on similar or related samples.

- **OSINT search is available on a "code block level"**, i.e., for files and process memory regions.

Technically, we do this by continuously retrieving OSINT reports, extracting the hashes, downloading the samples that correspond to these hashes, and indexing the code of malware samples into our malware database. We then use our code search engine to match code regions under investigation to OSINT samples.



3. Connect unknown to OSINT

Blogpost about malware family X, mentioning malware by hash

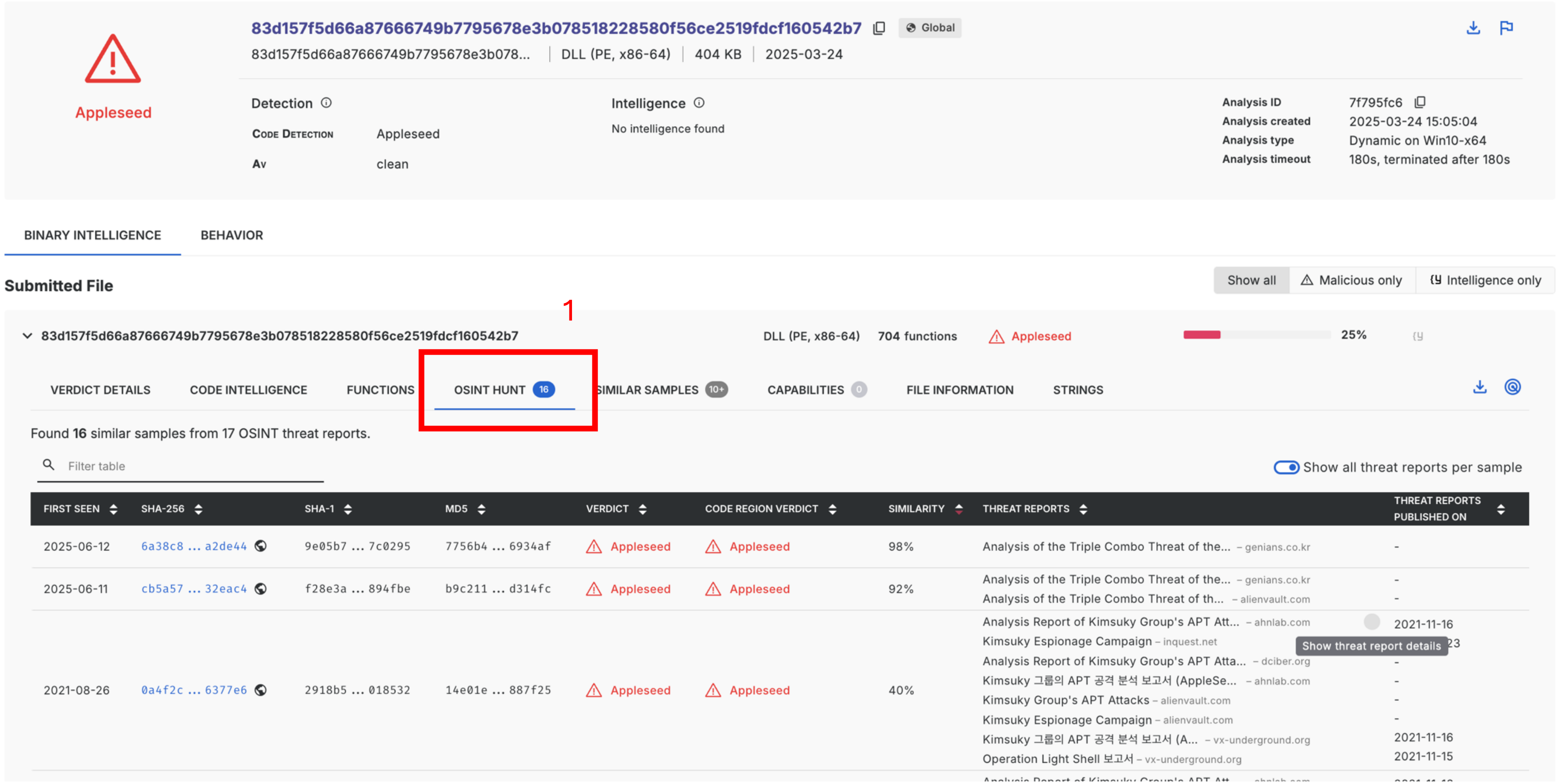
2.

1. Find code wise similar sample

Sample mentioned in blog post, retrieved by Threatray and indexed in our code database

Unknown malware under investigation

OSINT search example



83d157f5d66a87666749b7795678e3b078518228580f56ce2519fdcf160542b7 Global

83d157f5d66a87666749b7795678e3b078... | DLL (PE, x86-64) | 404 KB | 2025-03-24

Appleseed

Detection

Code Detection	Appleseed
Av	clean

Intelligence

No intelligence found

Analysis ID	7f795fc6
Analysis created	2025-03-24 15:05:04
Analysis type	Dynamic on Win10-x64
Analysis timeout	180s, terminated after 180s

BINARY INTELLIGENCE BEHAVIOR

Submitted File

Show all | Malicious only | Intelligence only

83d157f5d66a87666749b7795678e3b078518228580f56ce2519fdcf160542b7 DLL (PE, x86-64) 704 functions Appleseed 25%

VERDICT DETAILS | CODE INTELLIGENCE | FUNCTIONS | OSINT HUNT 16 | SIMILAR SAMPLES 10+ | CAPABILITIES 0 | FILE INFORMATION | STRINGS

Found **16** similar samples from 17 OSINT threat reports.

Filter table

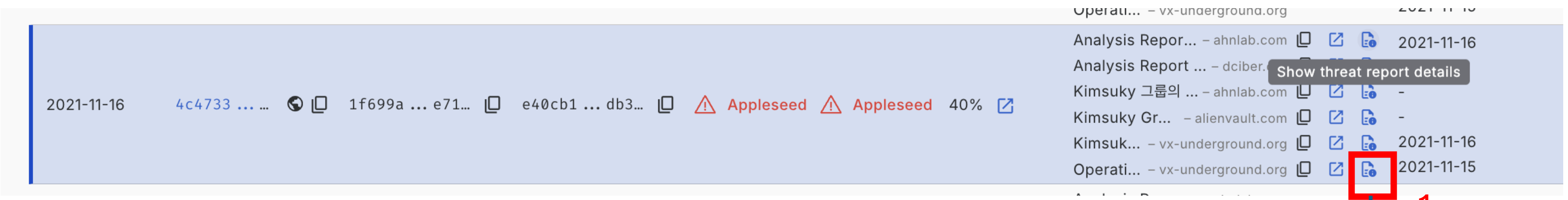
Show all threat reports per sample

FIRST SEEN	SHA-256	SHA-1	MD5	VERDICT	CODE REGION VERDICT	SIMILARITY	THREAT REPORTS	THREAT REPORTS PUBLISHED ON
2025-06-12	6a38c8 … a2de44	9e05b7 … 7c0295	7756b4 … 6934af	Appleseed	Appleseed	98%	Analysis of the Triple Combo Threat of the... – genians.co.kr	-
2025-06-11	cb5a57 … 32eac4	f28e3a … 894fbe	b9c211 … d314fc	Appleseed	Appleseed	92%	Analysis of the Triple Combo Threat of the... – genians.co.kr Analysis of the Triple Combo Threat of th... – alienvault.com	- -
2021-08-26	0a4f2c … 6377e6	2918b5 … 018532	14e01e … 887f25	Appleseed	Appleseed	40%	Analysis Report of Kimsuky Group's APT Att... – ahnlab.com Kimsuky Espionage Campaign – inquest.net Analysis Report of Kimsuky Group's APT Atta... – dciber.org Kimsuky 그룹의 APT 공격 분석 보고서 (AppleSe... – ahnlab.com Kimsuky Group's APT Attacks – alienvault.com Kimsuky Espionage Campaign – alienvault.com Kimsuky 그룹의 APT 공격 분석 보고서 (A... – vx-underground.org Operation Light Shell 보고서 – vx-underground.org	2021-11-16 23 - - - - 2021-11-16 2021-11-15

(1) The OSINT results are found in the OSINT tab of a code block

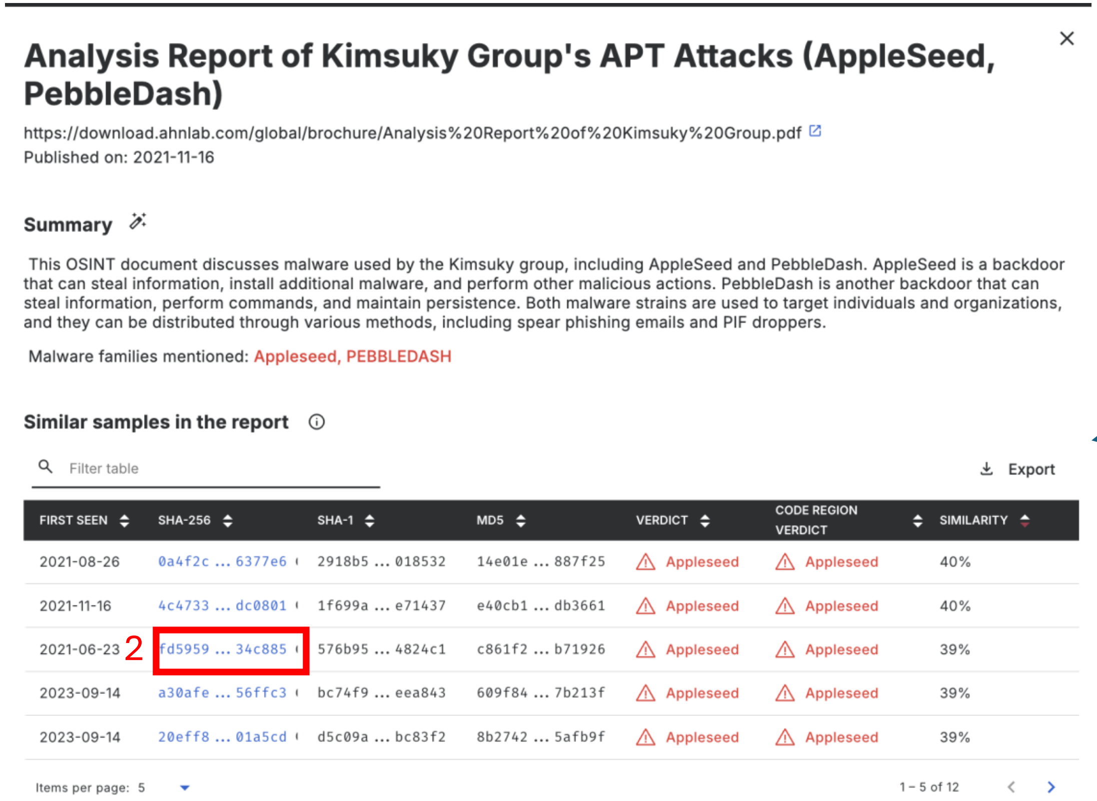
Each line line in the table is sample found in an OSINT report, that is similar to the code block under investigation

OSINT search example



2021-11-16 | 4c4733 ... ... | 1f699a ... e71... | e40cb1 ... db3... | ⚠ Appleseed | ⚠ Appleseed | 40%

Operati... – vx-underground.org	
Analysis Repor... – ahnlab.com	2021-11-16
Analysis Report ... – dciber.	
Kimsuky 그룹의 ... – ahnlab.com	-
Kimsuky Gr... – alienvault.com	-
Kimsuk... – vx-underground.org	2021-11-16
Operati... – vx-underground.org	2021-11-15



Analysis Report of Kimsuky Group's APT Attacks (AppleSeed, PebbleDash)

https://download.ahnlab.com/global/brochure/Analysis%20Report%20of%20Kimsuky%20Group.pdf

Published on: 2021-11-16

Summary

This OSINT document discusses malware used by the Kimsuky group, including AppleSeed and PebbleDash. AppleSeed is a backdoor that can steal information, install additional malware, and perform other malicious actions. PebbleDash is another backdoor that can steal information, perform commands, and maintain persistence. Both malware strains are used to target individuals and organizations, and they can be distributed through various methods, including spear phishing emails and PIF droppers.

Malware families mentioned: Appleseed, PEBBLEDASH

Similar samples in the report

FIRST SEEN	SHA-256	SHA-1	MD5	VERDICT	CODE REGION VERDICT	SIMILARITY
2021-08-26	0a4f2c ... 6377e6	2918b5 ... 018532	14e01e ... 887f25	⚠ Appleseed	⚠ Appleseed	40%
2021-11-16	4c4733 ... dc0801	1f699a ... e71437	e40cb1 ... db3661	⚠ Appleseed	⚠ Appleseed	40%
2021-06-23	fd5959 ... 34c885	576b95 ... 4824c1	c861f2 ... b71926	⚠ Appleseed	⚠ Appleseed	39%
2023-09-14	a30afe ... 56ffc3	bc74f9 ... eea843	609f84 ... 7b213f	⚠ Appleseed	⚠ Appleseed	39%
2023-09-14	20eff8 ... 01a5cd	d5c09a ... bc83f2	8b2742 ... 5afb9f	⚠ Appleseed	⚠ Appleseed	39%

Items per page: 5

1 – 5 of 12

(1) Click on the “Show threat report details icon to open a report summary.

Here we show all samples we were able to retrieve from the report, including their classification.

(2) By clicking on the blue hash, you can pivot to any of them.

OSINT search example

- **Summary of the Appleseed example:**
  - Through OSINT search we find a blog post by Ahnlabs on the Appleseed family, used by Kimsuky actor.
    The report contains rich information, we quickly learn important details about the actor and two malware families, PebbleDash and Appleseed. We also learn that there is HTTP and SMTP version of Appleseed.
  - By searching for the hashes of the similar samples in the report (using normal text find), we quickly learn that our sample is similar to HTTP versions of Appleseed.
  - We find in the report a common URL pattern used “`/?m=a&p1=[PcID]&p2=[PcInfo]- [MalwareVersion]`”.
  - We go back to our sample to the ”Strings Tab” and find the the “`/?m=`“ string in the sample under investigation, which definitely confirms that we’re dealing with an Appleseed sample.
  - We can also use the URL pattern search `url:"*/?m=b&p1=*`” and pivot to many more sample in our global repository.

Code retro-hunts

- **What is code retro-hunt?** It is a unique search feature in Threatray, that allows to “search for similar code”.
  The feature starts from any code-block in the sample under investigation and finds samples that are code wise similar (more precisely: it finds analyses that contain a similar code block).

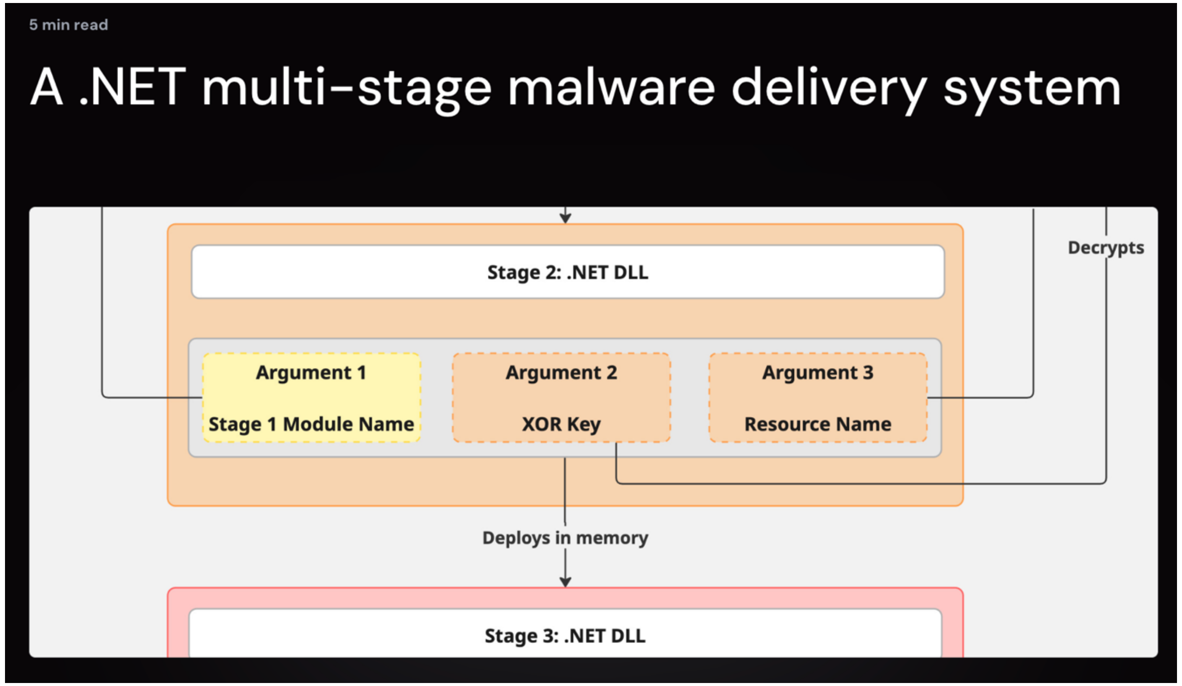
- **Fast code pivots.** Traditional tech like VT use YARA to search for similar code. This approach has its merits, but it takes time and skill. Threatray is point and click, thanks to our native code search capabilities.

- **Why is it useful?** It is feature that has many applications, but also and advanced feature, since depending on what code you hunt for the results, and their interpretation are quite different. It takes time to learn and appreciate this feature. Some examples:
  - **Pivot to similar samples,** e.g., when you need multiple samples from same family for YARA rule development, to find common IPs used, etc.
  - **Relate samples from different investigations** in your private repository
  - **Intelligence investigations of droppers and downloaders**
  - **Finding that an APT is always using the same libraries or other code components**
  - ….
- **Retro-hunt is available on a ”code block level”**, i.e., for files and process memory.

Code retro-hunt example

- In this example we are using the code-retro hunt investigate a loader and find out what malware it is dropping.

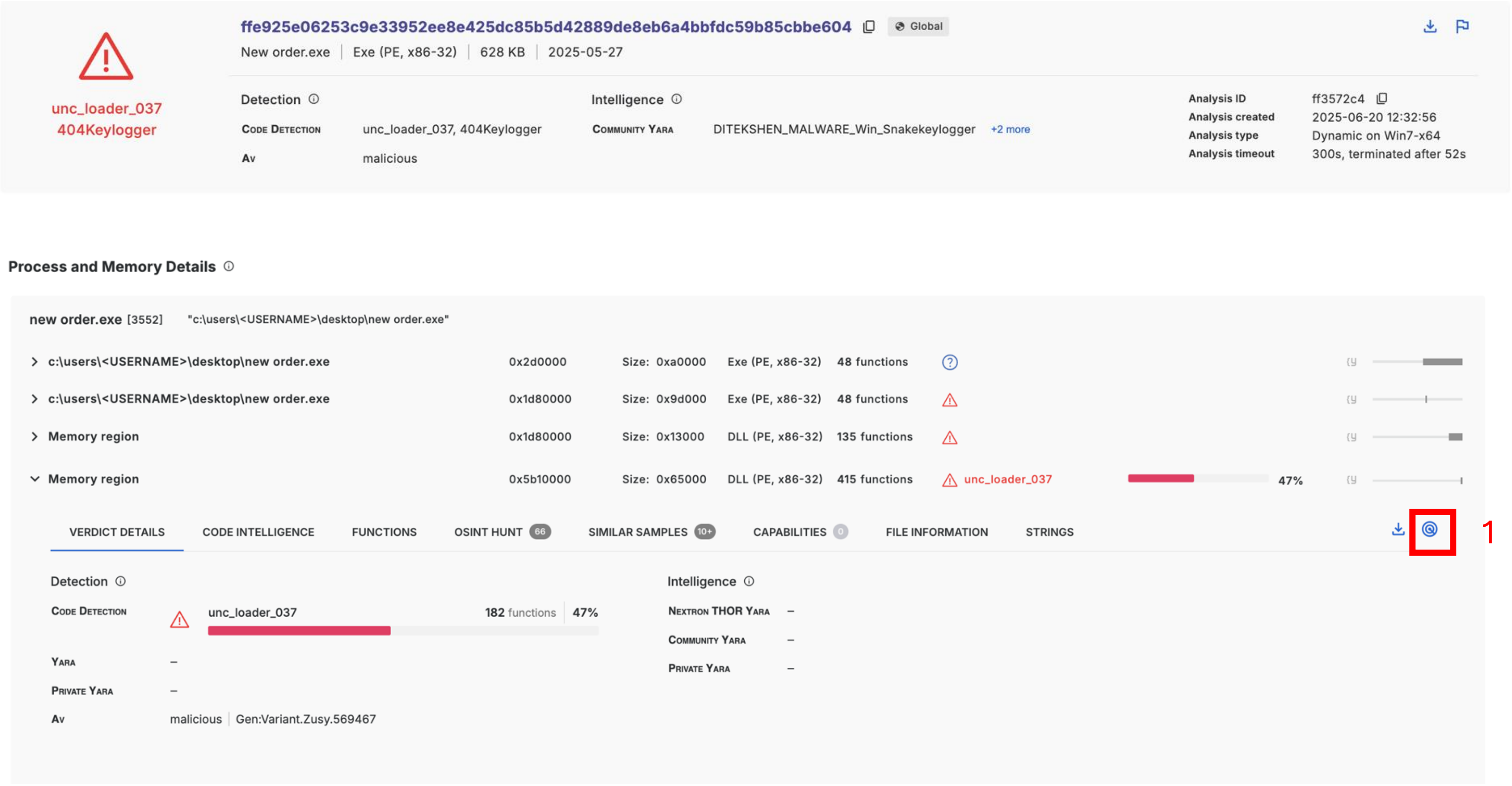
- It is a real-world example in the sense that we have discovered a previously unknown malware loader, see blog post here: https://www.threatray.com/blog/a-net-multi-stage-malware-delivery-system



5 min read

A .NET multi-stage malware delivery system

Code retro-hunt example



unc_loader_037
404Keylogger

ffe925e06253c9e33952ee8e425dc85b5d42889de8eb6a4bbfdc59b85cbbe604 | Global

New order.exe | Exe (PE, x86-32) | 628 KB | 2025-05-27

Detection
- Code Detection: unc_loader_037, 404Keylogger
- Av: malicious

Intelligence
- Community Yara: DITEKSHEN_MALWARE_Win_Snakekeylogger +2 more

Analysis ID	ff3572c4
Analysis created	2025-06-20 12:32:56
Analysis type	Dynamic on Win7-x64
Analysis timeout	300s, terminated after 52s

Process and Memory Details

new order.exe [3552] "c:\users\<USERNAME>\desktop\new order.exe"

> c:\users\<USERNAME>\desktop\new order.exe	0x2d0000	Size: 0xa0000	Exe (PE, x86-32)	48 functions	?	
> c:\users\<USERNAME>\desktop\new order.exe	0x1d80000	Size: 0x9d000	Exe (PE, x86-32)	48 functions	⚠	
> Memory region	0x1d80000	Size: 0x13000	DLL (PE, x86-32)	135 functions	⚠	
⌄ Memory region	0x5b10000	Size: 0x65000	DLL (PE, x86-32)	415 functions	⚠ unc_loader_037	47%

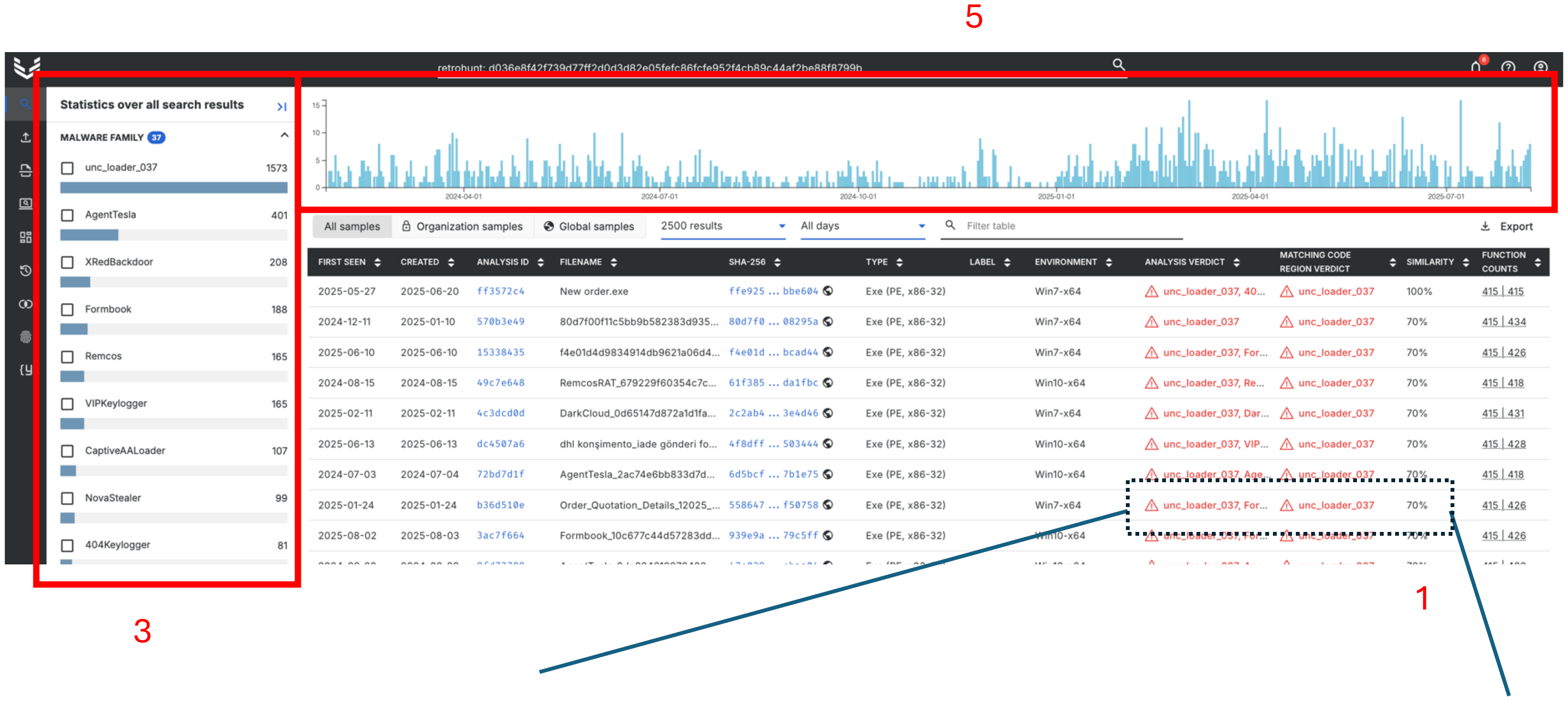
Detection
- Code Detection: ⚠ unc_loader_037 182 functions | 47%
- Yara: –
- Private Yara: –
- Av: malicious | Gen:Variant.Zusy.569467

Intelligence
- Nextron THOR Yara: –
- Community Yara: –
- Private Yara: –

We want to find samples that use a code wise similar loader to the "unc_loader_037" to better understand that loader.

(1) We click on the retro-hunt icon next to the code region ◎

Code retro-hunt example



retrohunt: d036e8f42f739d77ff2d0d3d82e05fefc86fcfe952f4cb89c44af2be88f8799b

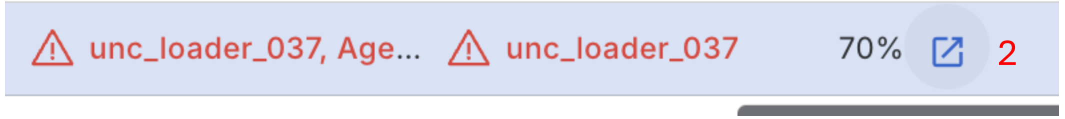
Statistics over all search results

MALWARE FAMILY 37

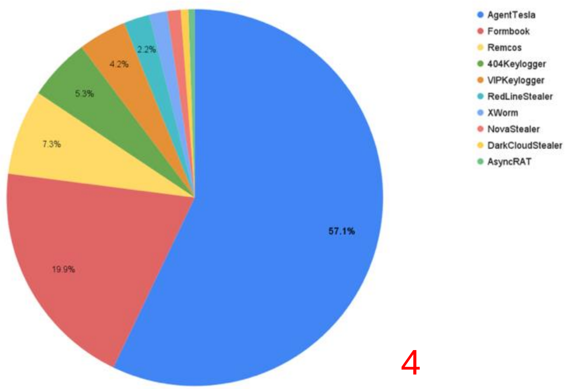
□ unc_loader_037	1573
□ AgentTesla	401
□ XRedBackdoor	208
□ Formbook	188
□ Remcos	165
□ VIPKeylogger	165
□ CaptiveAALoader	107
□ NovaStealer	99
□ 404Keylogger	81

All samples | Organization samples | Global samples | 2500 results | All days | Filter table | Export

FIRST SEEN	CREATED	ANALYSIS ID	FILENAME	SHA-256	TYPE	LABEL	ENVIRONMENT	ANALYSIS VERDICT	MATCHING CODE REGION VERDICT	SIMILARITY	FUNCTION COUNTS
2025-05-27	2025-06-20	ff3572c4	New order.exe	ffe925 ... bbe604	Exe (PE, x86-32)		Win7-x64	unc_loader_037, 40...	unc_loader_037	100%	415 | 415
2024-12-11	2025-01-10	570b3e49	80d7f00f11c5bb9b582383d935...	80d7f0 ... 08295a	Exe (PE, x86-32)		Win7-x64	unc_loader_037	unc_loader_037	70%	415 | 434
2025-06-10	2025-06-10	15338435	f4e01d4d9834914db9621a06d4...	f4e01d ... bcad44	Exe (PE, x86-32)		Win7-x64	unc_loader_037, For...	unc_loader_037	70%	415 | 426
2024-08-15	2024-08-15	49c7e648	RemcosRAT_679229f60354c7c...	61f385 ... da1fbc	Exe (PE, x86-32)		Win10-x64	unc_loader_037, Re...	unc_loader_037	70%	415 | 418
2025-02-11	2025-02-11	4c3dcd0d	DarkCloud_0d65147d872a1d1fa...	2c2ab4 ... 3e4d46	Exe (PE, x86-32)		Win7-x64	unc_loader_037, Dar...	unc_loader_037	70%	415 | 431
2025-06-13	2025-06-13	dc4507a6	dhl konşimento_iade gönderi fo...	4f8dff ... 503444	Exe (PE, x86-32)		Win10-x64	unc_loader_037, VIP...	unc_loader_037	70%	415 | 428
2024-07-03	2024-07-04	72bd7d1f	AgentTesla_2ac74e6bb833d7d...	6d5bcf ... 7b1e75	Exe (PE, x86-32)		Win10-x64	unc_loader_037, Age...	unc_loader_037	70%	415 | 418
2025-01-24	2025-01-24	b36d510e	Order_Quotation_Details_12025_...	558647 ... f50758	Exe (PE, x86-32)		Win7-x64	unc_loader_037, For...	unc_loader_037	70%	415 | 426
2025-08-02	2025-08-03	3ac7f664	Formbook_10c677c44d57283dd...	939e9a ... 79c5ff	Exe (PE, x86-32)		Win10-x64	unc_loader_037, For...	unc_loader_037	70%	415 | 426



unc_loader_037, Age... | unc_loader_037 | 70%



The search results look the same as when you use classical search – after all, retro-hunt is a search, a search for code.

(1) Unlike with classical search, we also show how code-wise similar the samples in the result set are.

Matches of 80%+ similarity are typically reliable, lower similarity can be helpful or not.

(2) You can pivot to any sample in the search results. The click will take you you to the *matching code block (!)* in the analysis of the samples.

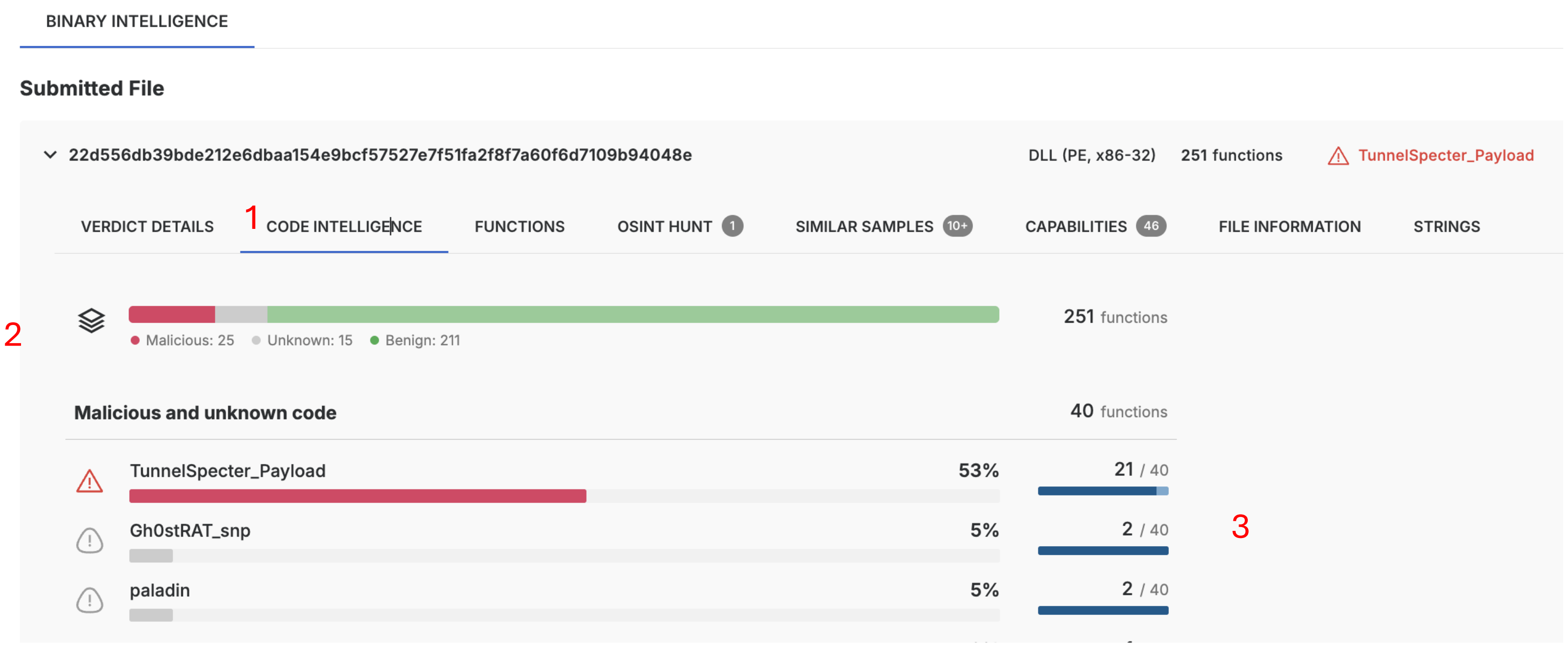
(3) The cluster stats show us which families are deployed by this loader: AgentTesla, XRedBackdoor, Formbook,…. This is how we produced the stats (4) in our blog.

(5) The timeline shows us that this loader has been active since beginning of 2024 → relevant loader to track.

THREATRAY

Code intelligence

Code intelligence (code DNA)



Submitted File

22d556db39bde212e6dbaa154e9bcf57527e7f51fa2f8f7a60f6d7109b94048e DLL (PE, x86-32) 251 functions TunnelSpecter_Payload

251 functions

● Malicious: 25 ● Unknown: 15 ● Benign: 211

Malicious and unknown code 40 functions

TunnelSpecter_Payload	53%	21 / 40
Gh0stRAT_snp	5%	2 / 40
paladin	5%	2 / 40

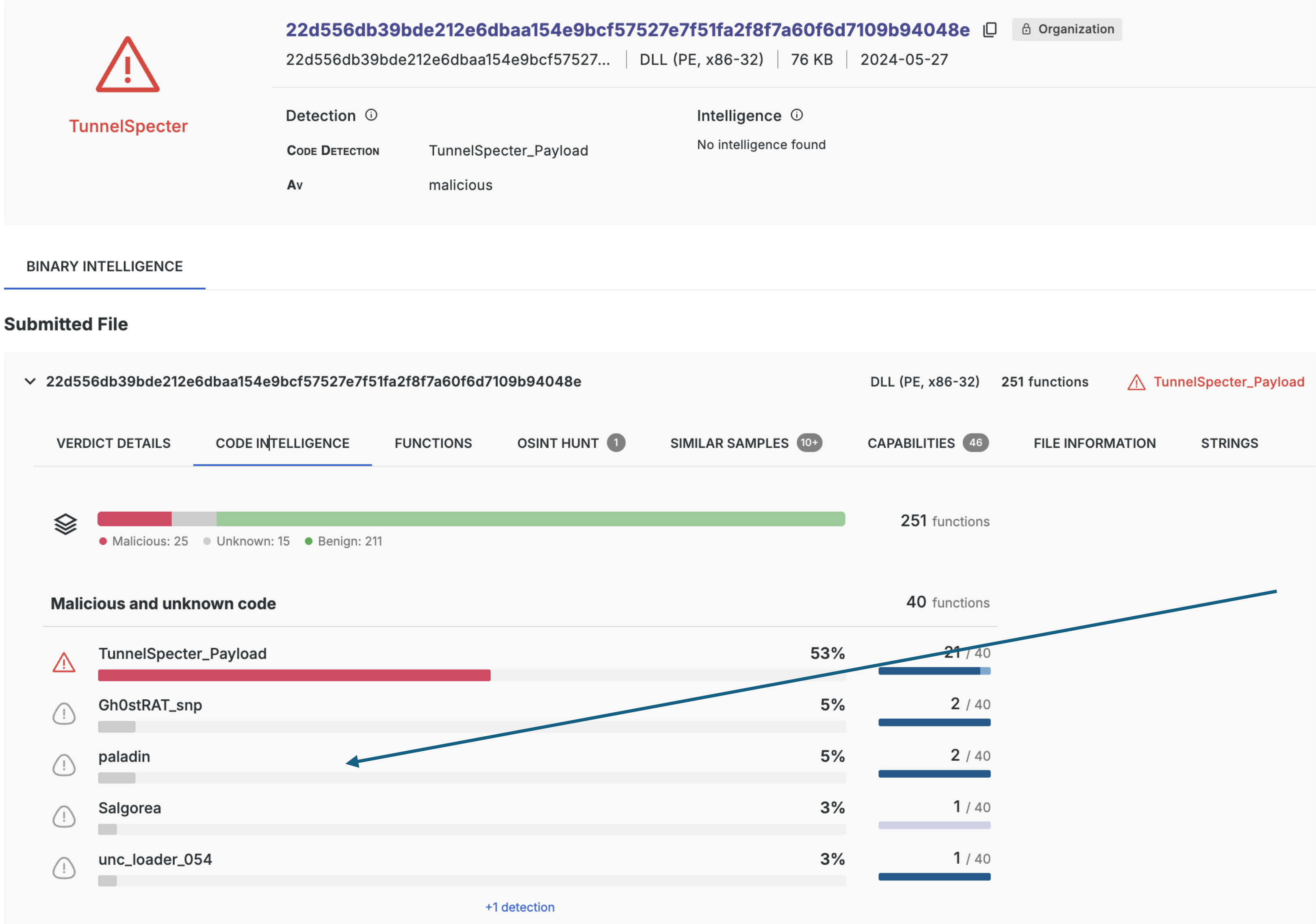
- (1) The code intelligence tab for each code block shows in detail the code composition of the that code block.

- (2) We distinguish malware code (red), unknown (grey) and green (benign). The stats are on a per function granularity, i.e., we attribute functions to families.

- (3) We also show how confident we are we the matches. Moreover, since we match by similarity, a few matches are often noise / useless, the more functions match the more reliable.

- This is an advanced feature, which is useful in some cases that matter, but less useful in others. Also, it might require further analysis in IDA pro (see next session)

Code intelligence (code DNA) – Example Chinese APT



TunnelSpecter

22d556db39bde212e6dbaa154e9bcf57527e7f51fa2f8f7a60f6d7109b94048e

22d556db39bde212e6dbaa154e9bcf57527... | DLL (PE, x86-32) | 76 KB | 2024-05-27

Detection

Code Detection	TunnelSpecter_Payload
Av	malicious

Intelligence

No intelligence found

Submitted File

22d556db39bde212e6dbaa154e9bcf57527e7f51fa2f8f7a60f6d7109b94048e DLL (PE, x86-32) 251 functions TunnelSpecter_Payload

● Malicious: 25 ● Unknown: 15 ● Benign: 211

251 functions

Malicious and unknown code 40 functions

TunnelSpecter_Payload	53%	21 / 40
Gh0stRAT_snp	5%	2 / 40
paladin	5%	2 / 40
Salgorea	3%	1 / 40
unc_loader_054	3%	1 / 40

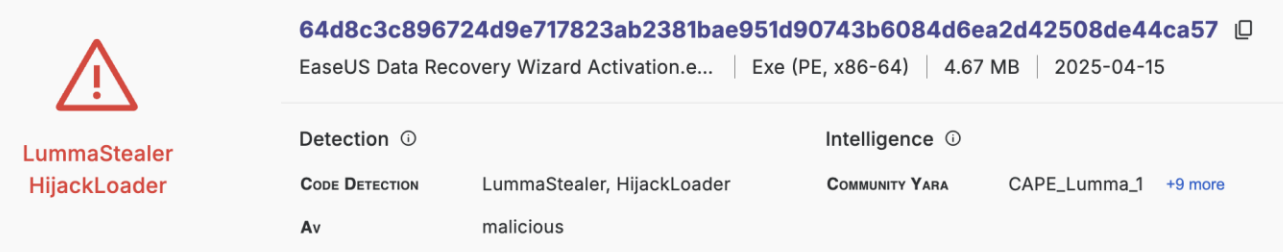
+1 detection

This is a sample we were investigating. Initially, we didn't know that it is TunnelSpectre.

But the code fragments from Gh0stRAT, paladin etc. put us on the China track.

Also it seems to indicate that the developers of these tools share some code.

Code intelligence (code DNA) – Backdoored DLL

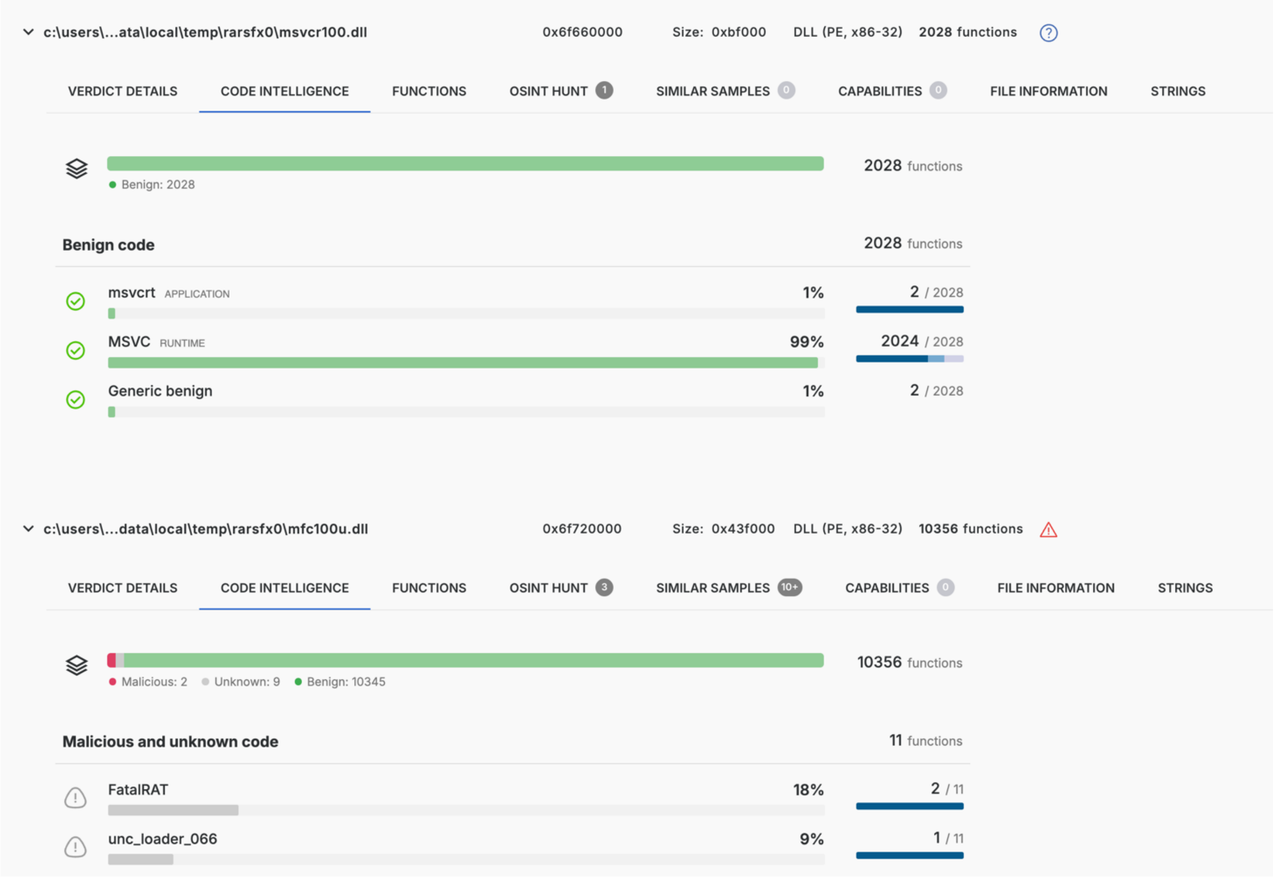


64d8c3c896724d9e717823ab2381bae951d90743b6084d6ea2d42508de44ca57

EaseUS Data Recovery Wizard Activation.e... | Exe (PE, x86-64) | 4.67 MB | 2025-04-15

LummaStealer
HijackLoader

Detection		Intelligence	
Code Detection	LummaStealer, HijackLoader	Community Yara	CAPE_Lumma_1 +9 more
Av	malicious		



c:\users\...ata\local\temp\rarsfx0\msvcr100.dll 0x6f660000 Size: 0xbf000 DLL (PE, x86-32) 2028 functions

2028 functions

● Benign: 2028

Benign code — 2028 functions

msvcrt	APPLICATION	1%	2 / 2028
MSVC	RUNTIME	99%	2024 / 2028
Generic benign		1%	2 / 2028

c:\users\...data\local\temp\rarsfx0\mfc100u.dll 0x6f720000 Size: 0x43f000 DLL (PE, x86-32) 10356 functions

10356 functions

● Malicious: 2 ● Unknown: 9 ● Benign: 10345

Malicious and unknown code — 11 functions

FatalRAT	18%	2 / 11
unc_loader_066	9%	1 / 11

Sample drops multiple of DLLs (can be seen in dynamic analysis file operations).

In the code intelligence tab, we see that some of the DLLs are 100% benign (1) and others are mostly benign but contain 9 unknown functions (2).

Using manual analysis in IDA pro we found that these 9 functions are malware code.

How to replay in your Threatray instance

Here are the analysis IDs for the examples shown:

- For the Latrodectus “running” mutex
  1a3ee1f5-94b9-457b-bc50-a8ce85e2ceb1

- For the Appleseed APT OSINT example, we have used analysis
  7f795fc6-0892-40d5-a5c2-5e1e38528b0e

- For the 404Keylogger loader retro-hunt we have used
  ff3572c4-1893-4a35-818f-ebcbde33b092

- For the code intelligence example on Chinese APT we have used
  c31bb52d-7a29-4c27-8e57-eb69ac1e1bb5

- For the code of the LummaStealer backdoored DLL we have used
  5c705269-e076-4ad2-bfa8-1a514ce08dbf