

Quick Guide to TI Lookup

About TI Lookup

Threat Intelligence Lookup is a fast tool that simplifies cyber threat investigations through flexible searches for Indicators of Compromise (IOCs), Indicators of Attack (IOAs), and Indicators of Behavior (IOBs).

TI Lookup equips you with effective research tools, helping you:

- ✓ Investigate and gather extensive and in-depth information on emerging and persistent cyber threats with speed.
- ✓ Receive real-time updates on your search queries.
- ✓ Enrich your threat intelligence with relevant context, indicators, and samples, manually analyzed by our team of threat analysts.
- ✓ Access a constantly updated database of threat data, collected from millions of public malware and phishing samples uploaded to ANY.RUN's Interactive Sandbox by a global community of 500,000 security professionals.

Key Features:



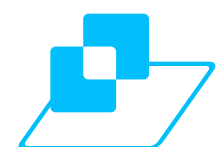
Easy and flexible search with over 40 search parameters, including IPs, hashes, registry keys, and processes



Real-time updates on new results related to your queries



Examples and context from other investigations to aid decision-making



Ability to combine indicators and events that are not directly related in one query to pinpoint specific threats



Access to data that is difficult or impossible to find in other sources

The screenshot shows the ANY RUN interface with a search query: `commandLine:"codigo" AND domainName:""`. The results are categorized into Domains (228) and Events (1171).

Domains 228

Date	Domain	Indicator
14 Nov, 2024	crib-endanger.sbs	lumma_stealer
13 Nov, 2024	geoplugin.net	
12 Nov, 2024	gig.energymaxgrp.eu	vidar_stealer
5 Nov, 2024	bafkreidskhfvpc74azopnn5qu64etyo4mpi2da3yfgin2f6t4cznjplv6y.ipf	
5 Nov, 2024	ftp.stingatoareincendii.ro	agent_tesla
5 Nov, 2024	ankaraspotesya.com.tr	vidar_stealer
1 Nov, 2024	aarzoomarine.com	vidar_stealer

Events 1171

15 Nov, 2024

commandLine

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command \$Codigo
A9IDdBm2h0dHBz0i8nKycvMTAxJysnNy5maWxIbWFpbC5jb20vYXBpL2ZpbGUvZ2V0P
rJ3U0NXQ3QUxa1Znc2Q5JysncFQ5cGdTU2x2U3RHcm5USUNmRmhtVEtqM0xDNINRc

7620 powershell.exe "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -

stegocampaign 1539 4044

Types of Searches in TI Lookup



Single IOC Search:

This method allows you to look for a single indicator of compromise (IOC), such as a URL, MD5, SHA1, SHA256, IP, or domain name.



Events Search:

This method lets you search for specific events recorded during sandbox analysis, which may include launched processes, triggered Suricata rules, registry key modifications, command executions, mutexes, and more.



Combined Search:

This method enables you to combine IOCs or events that were discovered together within an analytical session (sandbox task). These can be associated with the same or different activities or stages of the investigation.



Wildcard Search:

To enhance the flexibility and precision of your searches, you can utilize wildcards such as the asterisk (*), caret (^), dollar sign (\$), and question mark (?). These symbols allow for broader or more specific queries.

Search Parameters in TI Lookup

Task

threatName

The name of a particular threat: malware family, threat type, etc., as identified by the sandbox.

threatName:“**Phishing**”

submissionCountry

The country from which the threat sample was submitted.

submissionCountry:“**es**”

taskType

The type of the sample submitted to the sandbox.

taskType:“**URL**”

threatLevel

A verdict on the threat level of the sample.

threatLevel:“**malicious**”

Registry

registryKey

The specific key within the registry hive where the modification occurred. Please note: when entering registry keys, use a double backslash (\) to escape the single backslash.

registryKey: **"Windows\\CurrentVersion\\RunOnce"**

registryName

The name of the Windows Registry key field.

registryName: **"browseinplace"**

registryValue

The value of the Windows Registry key.

registryValue: **"internet explorer\\iexplore.exe"**

Environment

os

The specific version of Windows used in the environment.

os:"11"

osSoftwareSet

The software package of applications installed on the OS.

osSoftwareSet:"clean"

osBitVersion

The bitness of the operating system, 32-bit or 64-bit.

osBitVersion:"32"

Detection

ruleName

The name of the detection rule.

ruleName:“**Executable content was dropped or overwritten**”

ruleThreatLevel

The threat level assigned to a particular event.

ruleThreatLevel:“**malicious**”

MITRE

Techniques used by the malware according to the MITRE ATT&CK classification.

MITRE:“**T1071**”

Module

moduleImagePath

The full path to the module's image file, the location on the disk where the module's executable is stored.

moduleImagePath:“**SysWOW64\\cryptbase.dll**”

Connection

domainName

The domain name that was recorded during the threat execution in a sandbox.

domainName: **"twentyvd20sb.top"**

destinationIP

The IP address of the network connection that was established or attempted.

destinationIP: **"147.185.221.22"**

destinationPort

The network port through which the connection was established.

destinationPort: **"49760"**

destinationIpAsn

Detected ASN.

destinationIpAsn: **"akamai-as"**

destinationIPgeo

Two-letter country or region code of the detected IP geolocation.

destinationIPgeo: **"ae"**

ja3, ja3s, jarm

Types of TLS fingerprints that can indicate certain threats.

ja3s: **"1af33e1657631357c73119488045302c" (JA3S)**

Process

imagePath

Full path to process image.

imagePath: "System32\\conhost.exe"

commandLine

Full command line that initiated the process.

commandLine: "PDQConnectAgent\\pdq-connect-agent.exe -service"

injectedFlag

Indication of whether a process has been injected.

injectedFlag: "true"

Network threat

suricataMessage

The description of the threat according to Suricata.

suricataMessage: "ET INFO 404/Snake/Matiex Keylogger Style External IP Check"

suricataClass

The category assigned to the threat by Suricata based on its characteristics.

suricataClass: "a network trojan was detected"

suricataID

The unique identifier of the Suricata rule.

suricataID: "2044767"

suricataThreatLevel

The verdict on the threat according to Suricata based on its potential impact.

suricataThreatLevel: "malicious"

File

filePath

The full path to the file on the system.

filePath: **"invoice"**

fileEventPath

The path of a file associated with a file event.

fileEventPath: **"factura"**

fileExtension

The extension that indicates the file type.

fileExtension: **"exe"**

Sha256, sha1, md5

Hash values relating to a file.

Sha256, sha1, md5: **"1412faf1bfd96e91340cedcea80ee09d"**

Synchronization

syncObjectName

The name or identifier of the synchronization object used.

syncObjectName: "rmc"

syncObjectType

The type of synchronization object used.

syncObjectType: "mutex"

syncObjectOperation

The operation performed on the synchronization object.

syncObjectOperation: "create"

URL

URL

The URL called by the process.

URL: `"http://192.168.37.128:8880/zv8u"`

HttpRequestContentType

The content type of the HTTP request sent to the server.

HttpRequestContentType: `"application/octet-stream"`

HttpResponseContentType

The content type of the HTTP response received from the server.

HttpResponseContentType: `"text/html"`

HttpRequestFileType

The file type of the file being uploaded in the HTTP request.

HttpRequestFileType: `"binary"`

HttpResponseFileType

The file type of the file being downloaded in the HTTP response.

HttpResponseFileType: `"binary"`

YARA Search

YARA Search is a core feature of TI Lookup. It allows users to scan ANY.RUN's threat intelligence database with their custom YARA rules to identify matching files.

✔ Rule Editor:

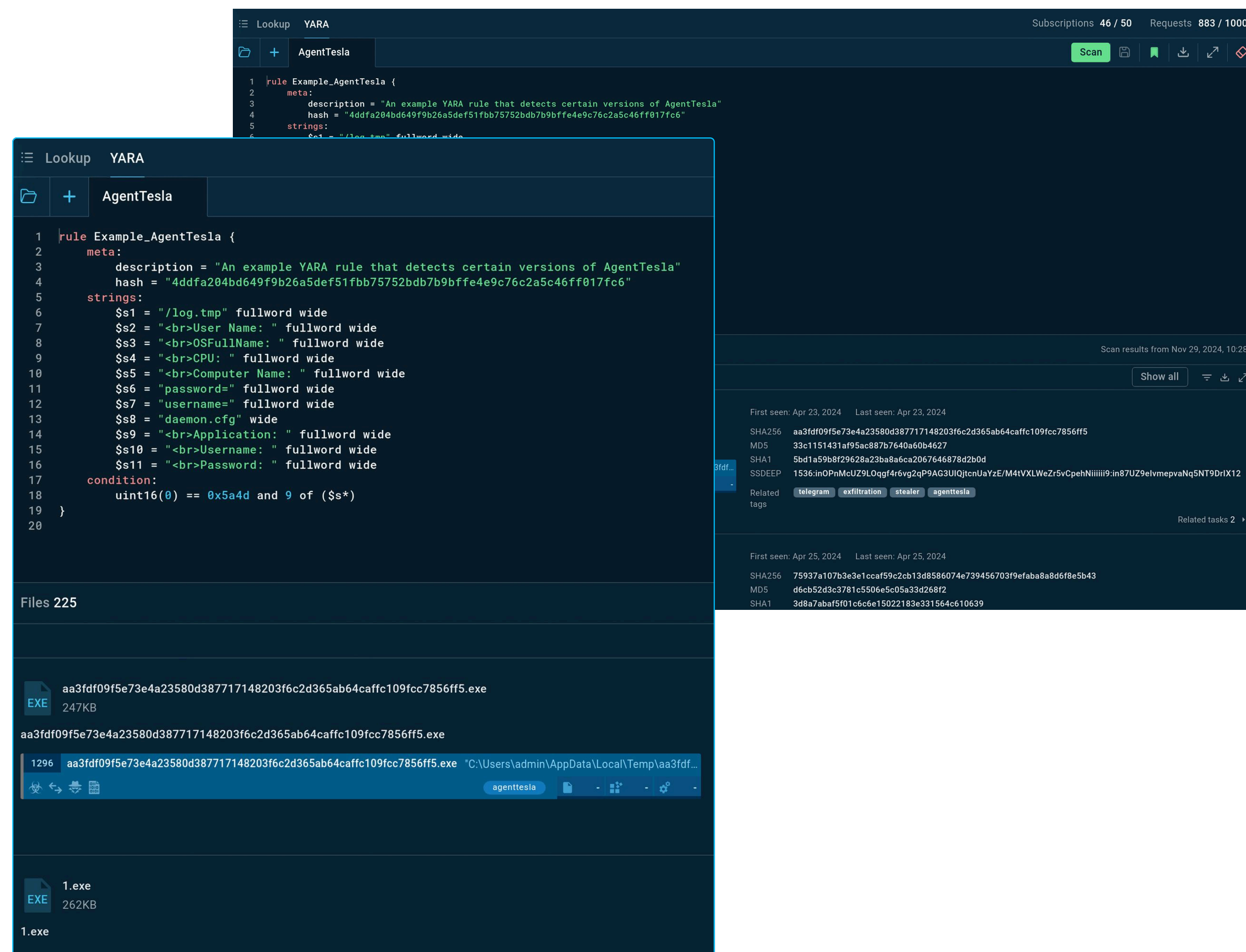
Create, edit, and manage YARA rules within TI Lookup using a built-in editor with syntax highlighting.

✔ Attack Analysis:

See how identified files operate in real-world attacks by exploring sandbox sessions.

✔ Efficient Search:

Run multiple searches in parallel, with initial results in under 5 seconds.



The screenshot displays the ANY.RUN YARA Search interface. At the top, there's a navigation bar with 'Lookup YARA', 'Subscriptions 46 / 50', and 'Requests 883 / 1000'. Below this is a search bar containing 'AgentTesla' and a 'Scan' button. The main area is divided into two panels. The left panel shows a YARA rule editor with the following code:

```

1 rule Example_AgentTesla {
2   meta:
3     description = "An example YARA rule that detects certain versions of AgentTesla"
4     hash = "4ddfa204bd649f9b26a5def51fbb75752bdb7b9bffe4e9c76c2a5c46ff017fc6"
5   strings:
6     $s1 = "/log.tmp" fullword wide
7     $s2 = "<br>User Name: " fullword wide
8     $s3 = "<br>OSFullName: " fullword wide
9     $s4 = "<br>CPU: " fullword wide
10    $s5 = "<br>Computer Name: " fullword wide
11    $s6 = "password=" fullword wide
12    $s7 = "username=" fullword wide
13    $s8 = "daemon.cfg" wide
14    $s9 = "<br>Application: " fullword wide
15    $s10 = "<br>Username: " fullword wide
16    $s11 = "<br>Password: " fullword wide
17   condition:
18     uint16(0) == 0x5a4d and 9 of ($s*)
19 }
20

```

The right panel shows search results for 'AgentTesla'. It includes a 'Scan results from Nov 29, 2024, 10:28' header and a 'Show all' button. Below this, there are two sections of results. The first section shows results from April 23, 2024, with columns for 'First seen', 'Last seen', 'SHA256', 'MD5', 'SHA1', and 'SSDEEP'. The second section shows results from April 25, 2024, with the same columns. Below the results, there are 'Related tags' (telegram, exfiltration, stealer, agenttesla) and 'Related tasks 2'. At the bottom, there's a 'Files 225' section with a list of files, including 'aa3dfd09f5e73e4a23580d387717148203f6c2d365ab64caffc109fcc7856ff5.exe' (247KB) and '1.exe' (262KB). A file viewer is open for the first file, showing its path and content.

Wildcard Characters

Asterisk (*)

Function

Represents any number of characters, including none.

How it is used

Replaces unknown parts in your query string. It's automatically added at the start and end of each query.

Example:

filePath:"invoice*.pdf"

Finds files with "invoice" and ".pdf" in the path. Invisible asterisks allow any characters before/after.

Caret (^)

Function Prevents matches with any characters before the specified query content.

How it is used Specifies that the content must appear at the start of the string.

Example: MITRE:"^T108" Finds all sandbox session (tasks) where the MITRE techniques starting with "T108" were identified.

Dollar sign (\$)

Function Excludes matches with any characters after the specified content.

How it is used Placed at the end to specify that the requested content ends the string.

Example:
filePath:"kill.cmd\$" Finds all files whose name ends with the text "kill.cmd".

Question mark (?)

Function

Represents any single character or its absence.

How it is used

Place the question mark (?) anywhere in the query string to replace a single unknown or variable character.

Example:

filePath:`"invoice*.doc?"`

This query will find files whose names contain "invoice" followed by any sequence of characters, then ".doc", and finally exactly one additional character.

Search Operators in TI Lookup

TI Lookup supports the use of logical operators AND, OR, and NOT, as well as grouping (with parentheses) for more complex search queries. This allows for greater flexibility and precision in your searches.

AND

Combines multiple conditions, requiring all of them to be true.

```
threatName:"vidar" AND url:".dll$"
```

OR

Combines multiple conditions, requiring at least one condition to be true.

```
threatName: syncObjectName:"DocumentUpdater" OR syncObjectName:"PackageManager"
```

NOT

Excludes results that match the specified condition.

```
commandLine:"Phishing" NOT taskType:"url"
```

Parentheses ()

Groups conditions to ensure they are processed first.

```
imagePath:"mshta.exe" AND (destinationPort:"80" OR destinationPort:"443")
```

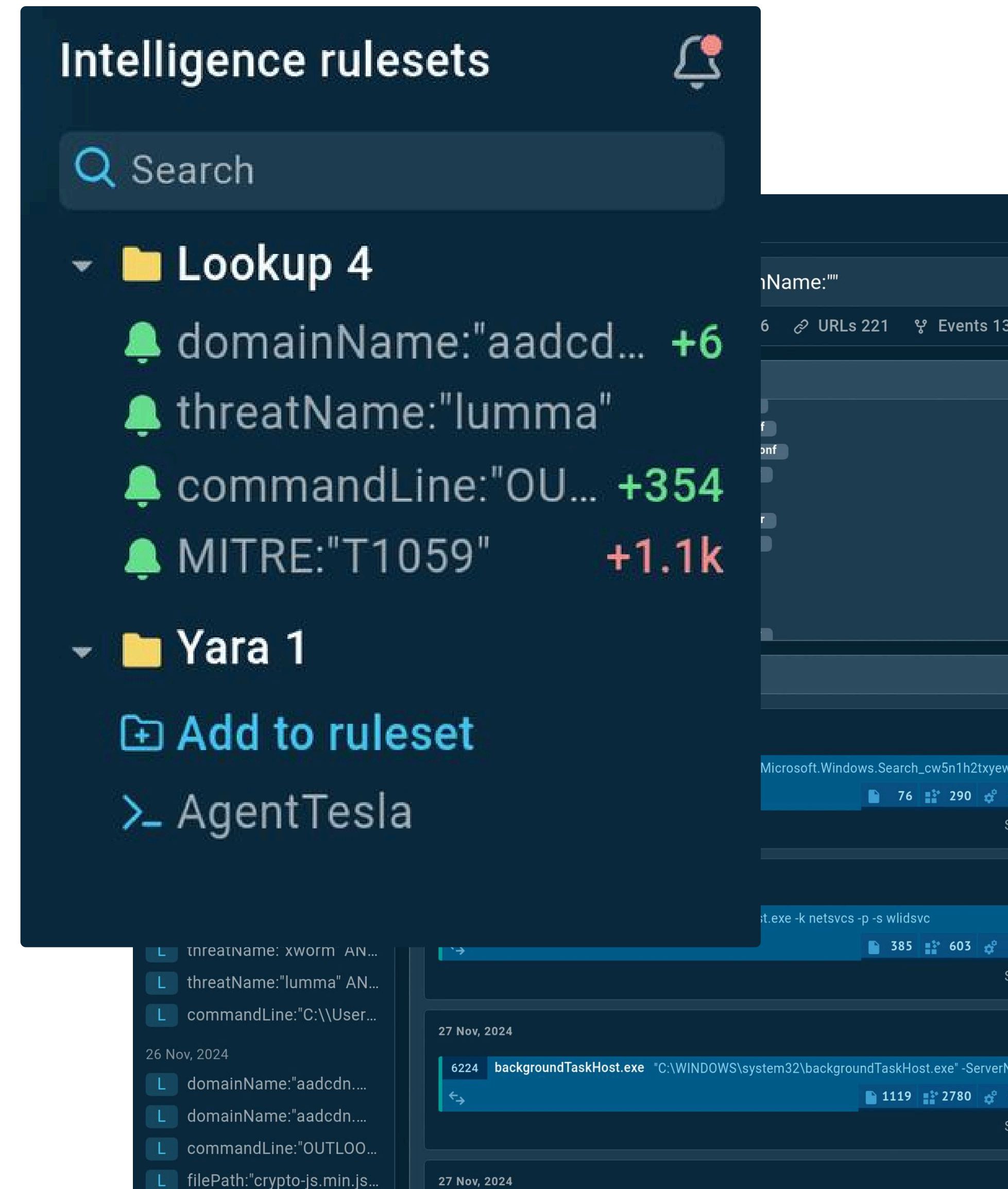
Notifications for Threat Intel Updates

TI Lookup delivers real-time updates on malware, phishing campaigns, and specific IOCs, IOAs, IOBs. To receive these, subscribe to notifications for new results related to your chosen queries.

How to subscribe:

- Enter a query you want to track.
Example: threatName:"lumma" AND submissionCountry:"es".
- Click the bell icon next to the search box to subscribe to the query.
- New subscription results will appear in the left sidebar.

Use the three dots menu next to each query to unsubscribe, pin, delete, or mark results as viewed.



The screenshot shows the 'Intelligence rulesets' section of the ANY RUN interface. It features a search bar at the top right with a bell icon. Below the search bar, there are two main categories: 'Lookup 4' and 'Yara 1'. Under 'Lookup 4', there are four queries, each with a bell icon and a count: 'domainName:"aadcd...' (+6), 'threatName:"lumma"' (no count), 'commandLine:"OU...' (+354), and 'MITRE:"T1059"' (+1.1k). Under 'Yara 1', there is one query. At the bottom, there is a button labeled 'Add to ruleset' and a link labeled 'AgentTesla'. The background shows a blurred view of the main interface with various data points and a terminal window.