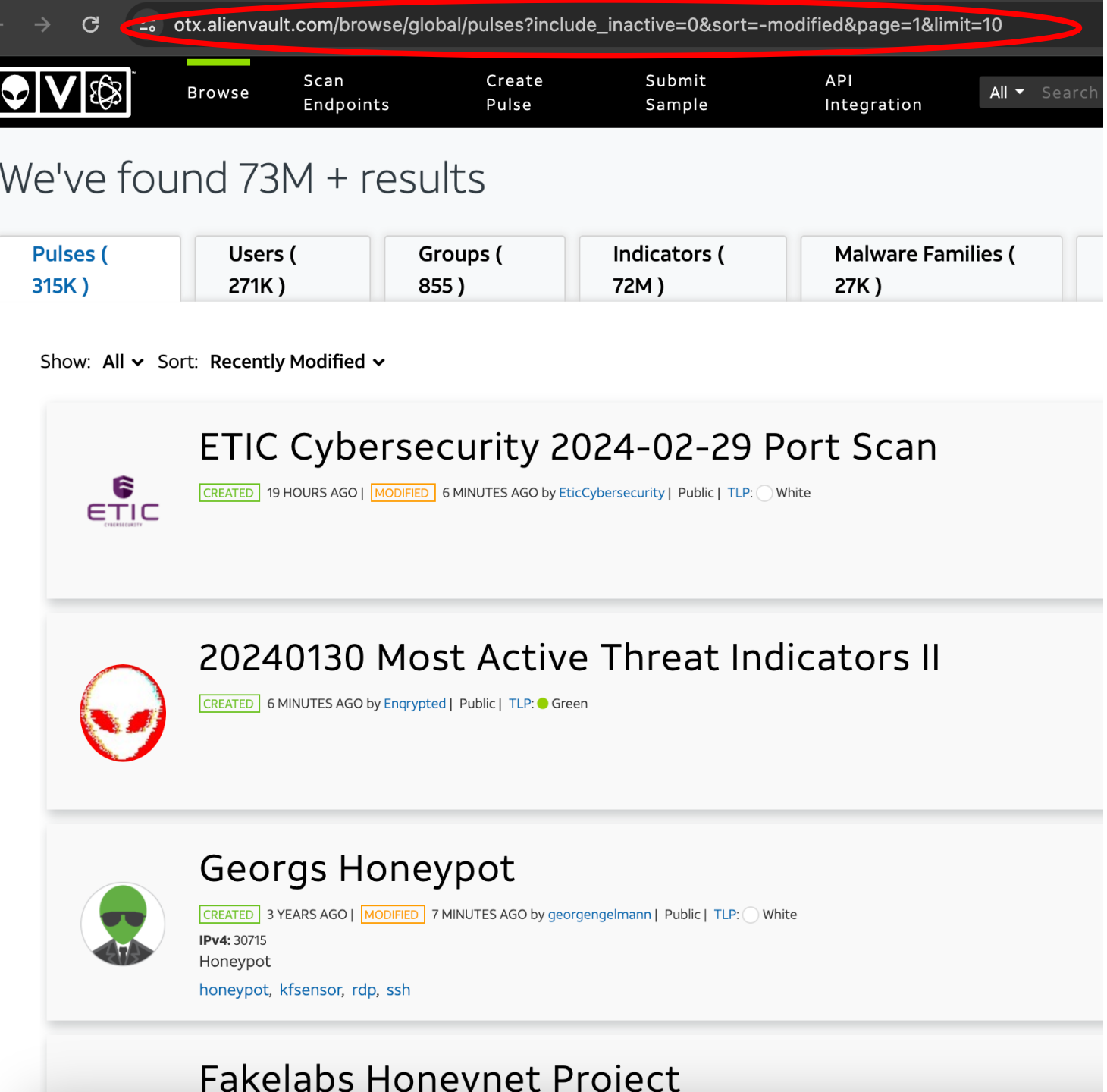
AlienVault OTX Insights

Mirai Botnet Indicators

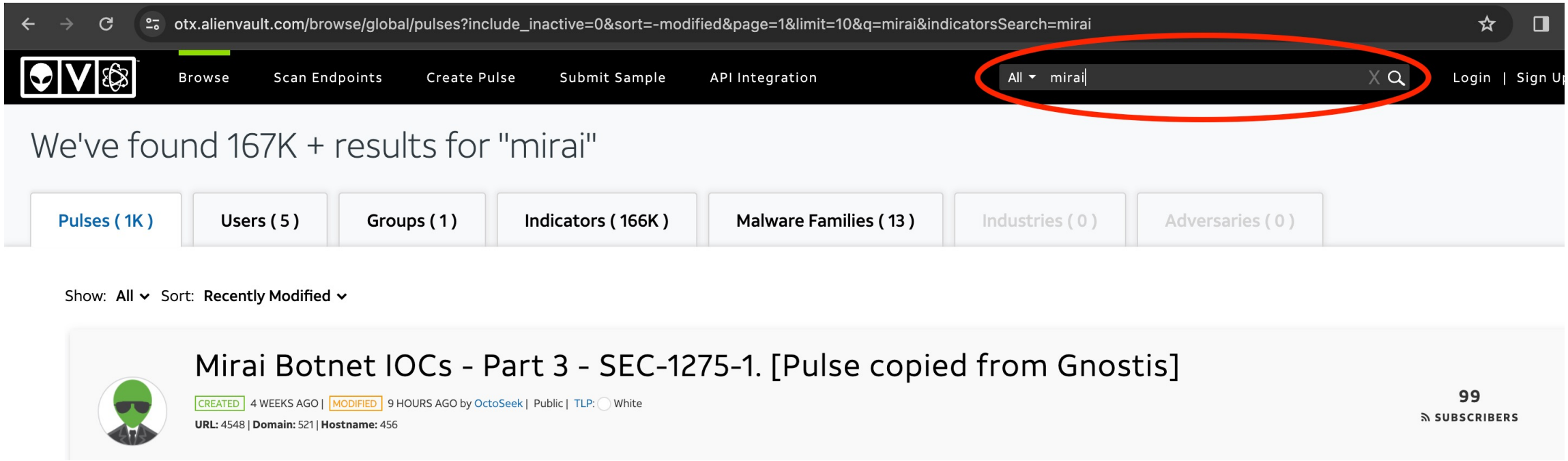


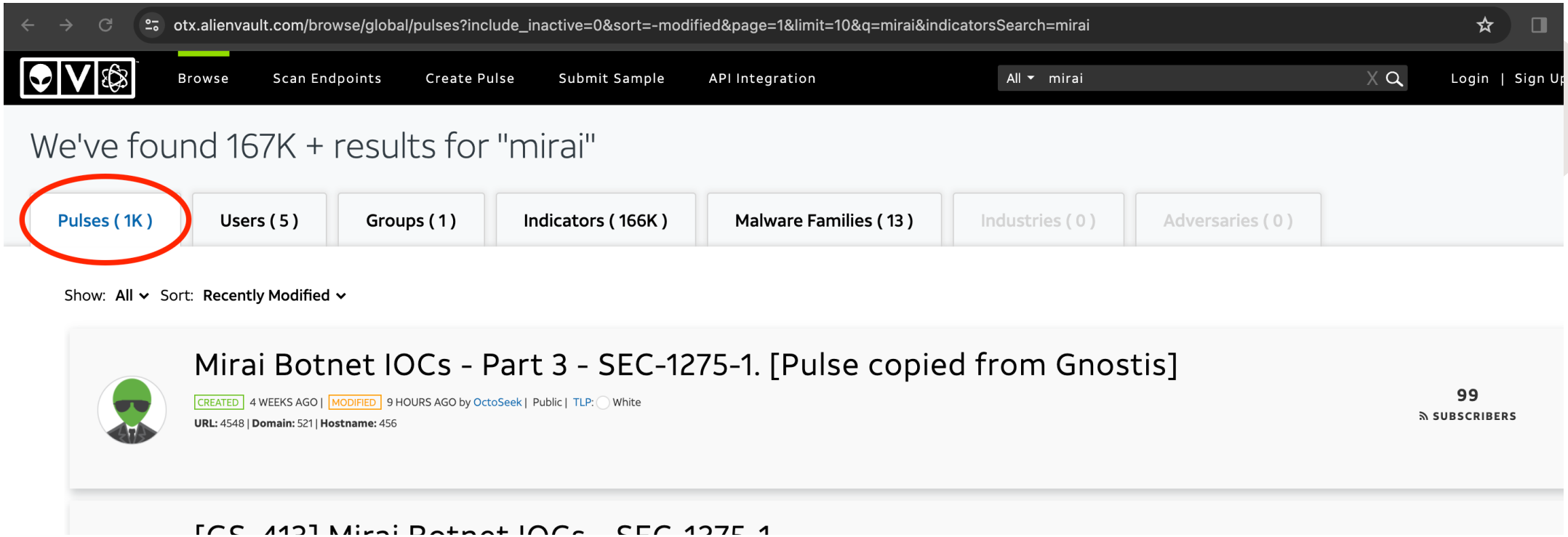
Accessing AlienVault OTX

Navigate to https://otx.alienvault.com/browse/global/pulses?include_inactive=0&sort=-modified&page=1&limit=10

Searching for Mirai

Type ”Mirai” into the ‘Search OTX’ field.





Understanding Pulses

Pulses are collections of IoCs related to cybersecurity threats.

Browse Scan Endpoints Create Pulse Submit Sample API Integration

Login | Sign Up

Mirai Botnet IOCs - Part 3 - SEC-1275-1. [Pulse copied from Gnostis]

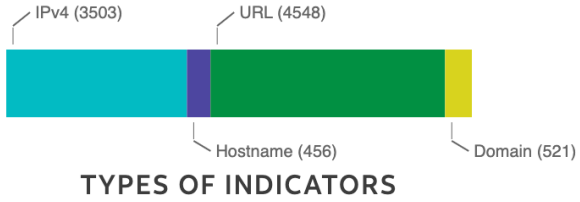
CREATED 4 WEEKS AGO | MODIFIED 9 HOURS AGO by OctoSeek | Public | TLP: White

REFERENCE: https://1275.ru/ioc/3029/mirai-botnet-iocs-part-3/

TAGS: mirai botnet, iocs, mirai, linux, compromise ipv4, domain port, combinations, gs003, gs005, gs008

ENDPOINT SECURITY Scan your endpoints for IOCs from this Pulse!

Indicators of Compromise (9K) | Related Pulses (1227) | Comments (0) | History (0)



TYPES OF INDICATORS

Show 10 entries

TYPE	INDICATOR	ROLE	TITLE
hostname	zxcxffyttygbbgfgf12121bot.duckdns.org		
hostname	zodiaclol.softether.net		
hostname	znet.whatareyousearchingfor.net		
hostname	zero.sudolite.ml		
hostname	yzykar.ddns.net		
hostname	yarunet.ddns.net		
hostname	y.fd6fq54s6df541q23sdxfg.eu		

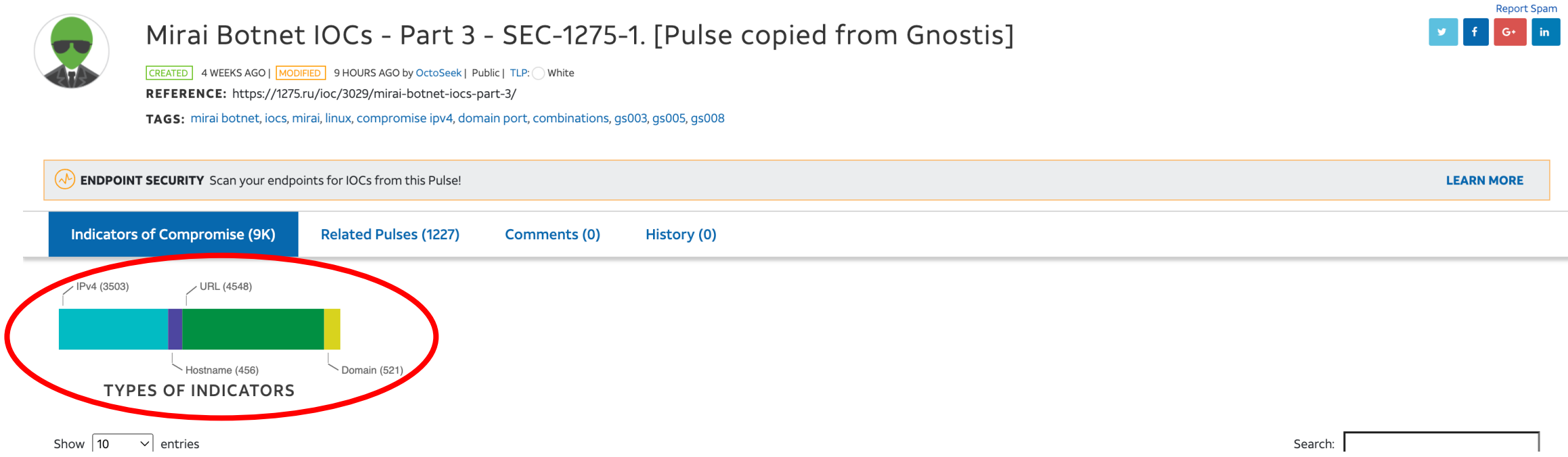
Selecting a Mirai Pulse

Select a Pulse with “Mirai” in the title, like ”Mirai Botnet IoCs.”

ADDED	ACTIVE	RELATED PULSES
Feb 3, 2024, 8:21:12 PM		2
Feb 3, 2024, 8:21:12 PM		1
Feb 3, 2024, 8:21:12 PM		2
Feb 3, 2024, 8:21:12 PM		1
Feb 3, 2024, 8:21:12 PM		6

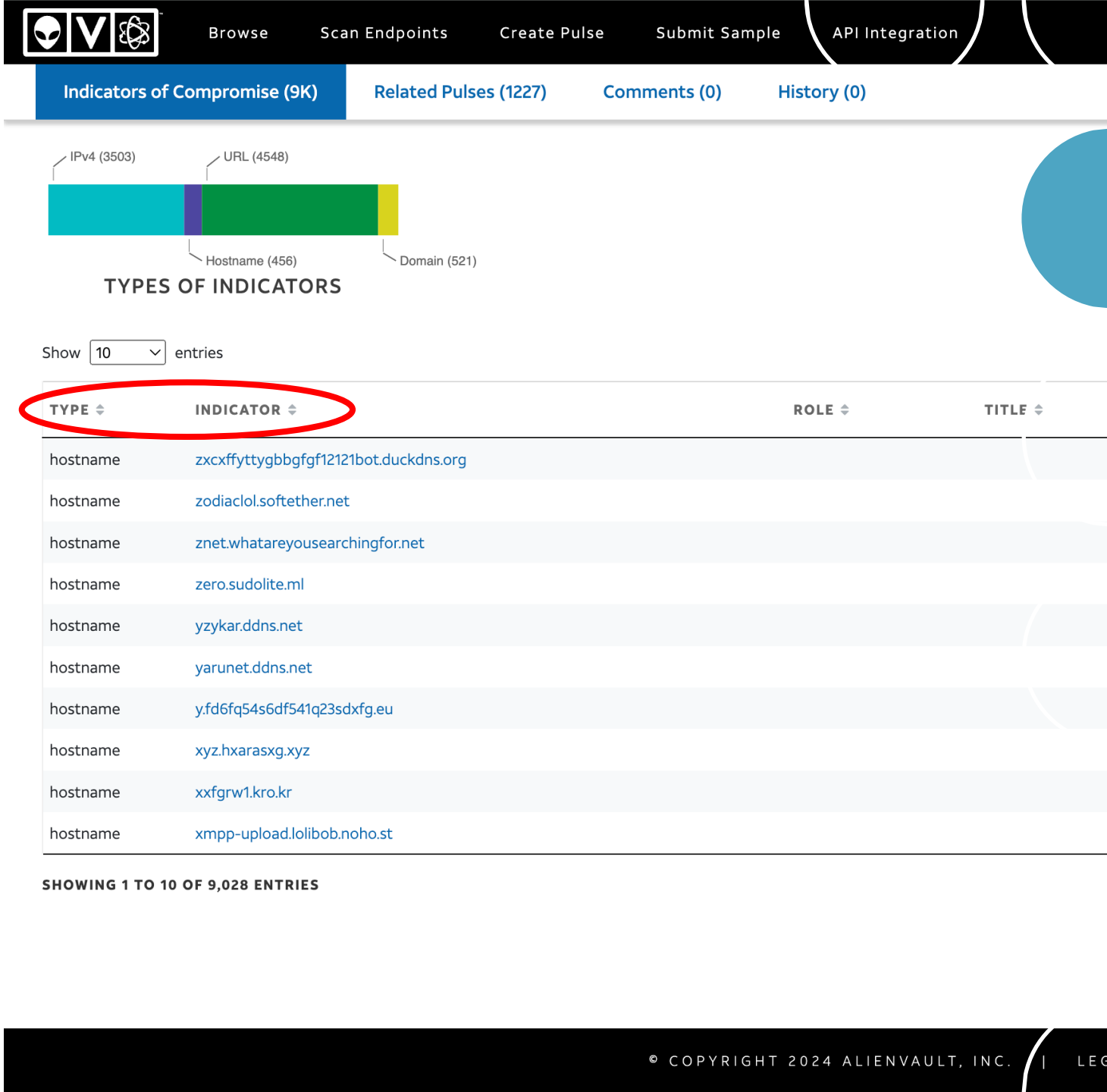
Examining Pulse Details

Observe the colored bar showing TYPES OF INDICATORS.



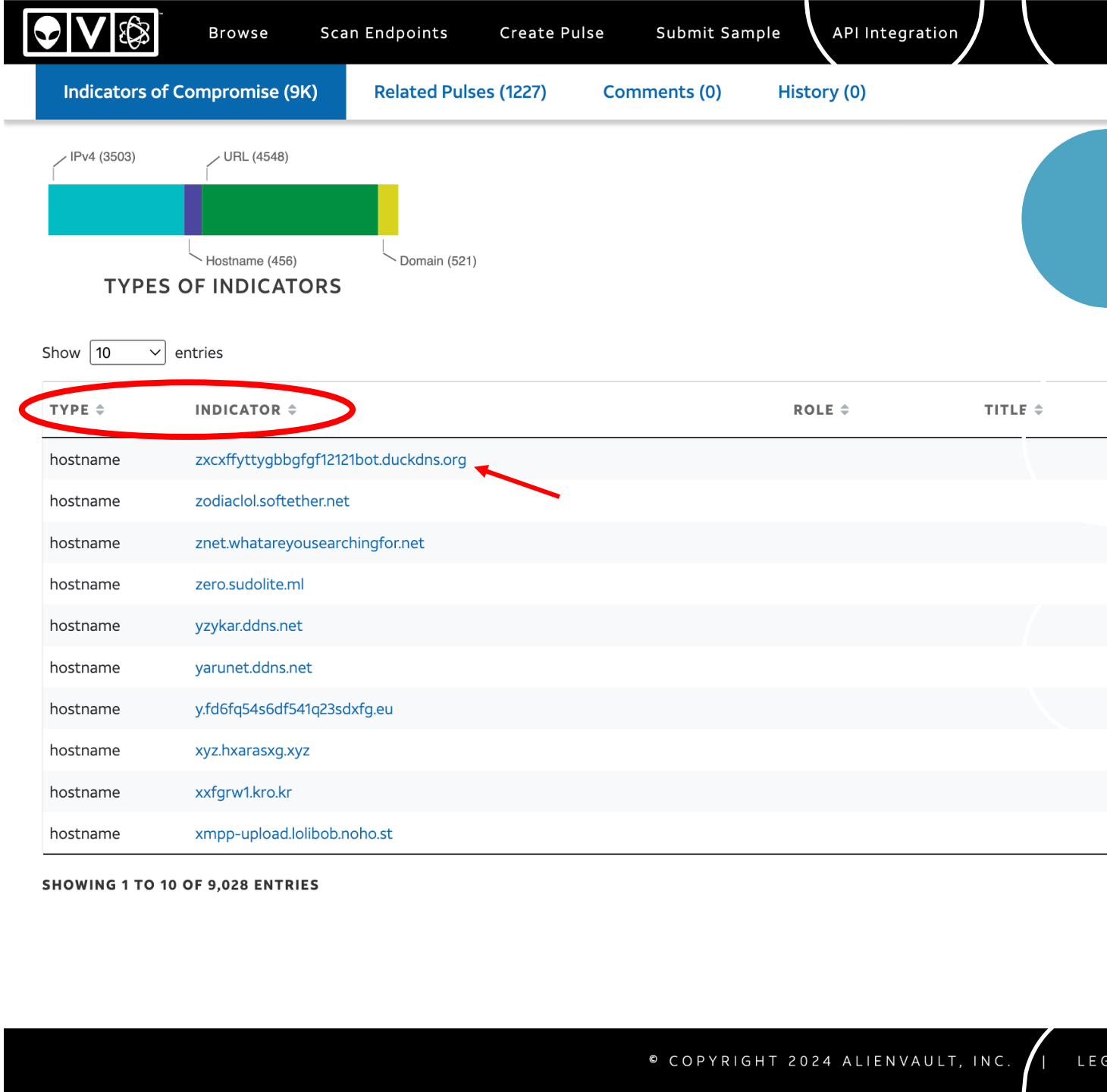
Identifying Indicator Types

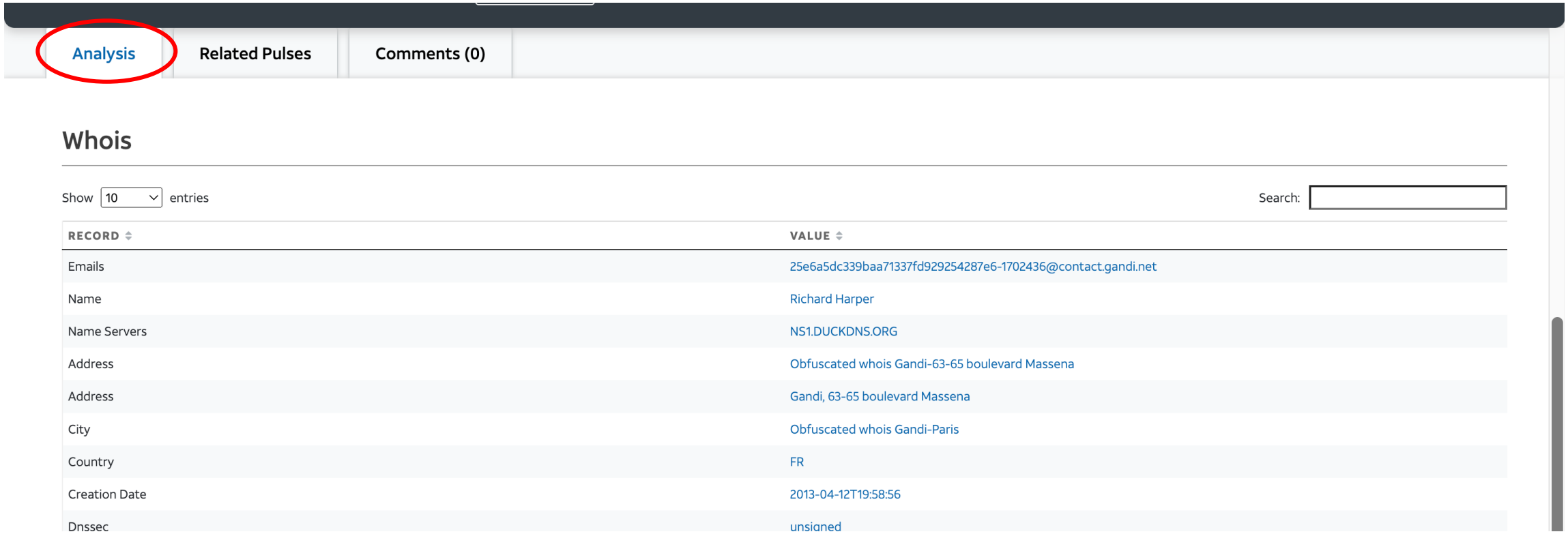
Note one of the indicator types, such as hostname, Domain or IP.



Exploring an Indicator

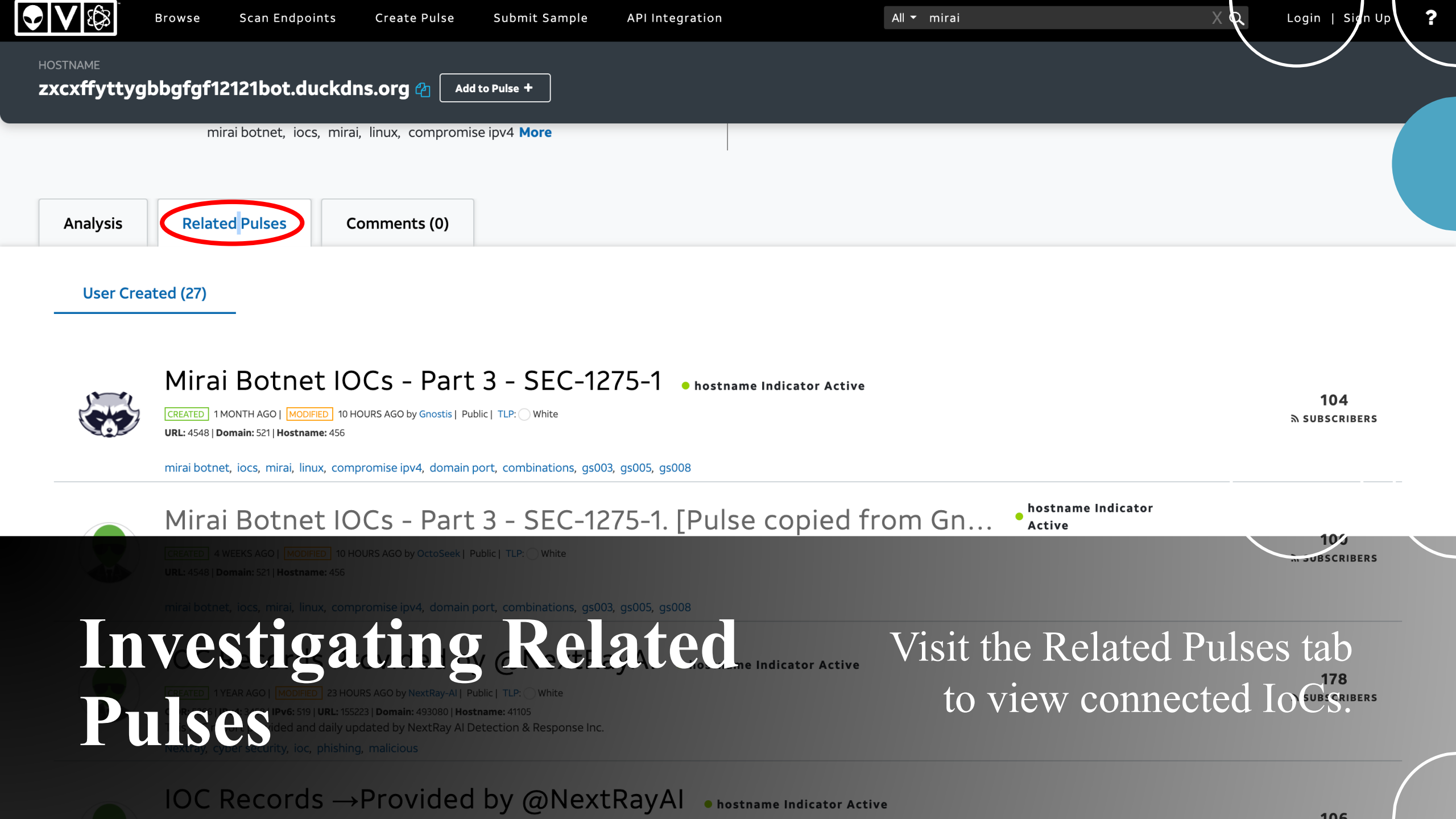
Click an item under INDICATOR to view its analysis.





Analyzing Indicator Details

Scroll through the analysis tab results.

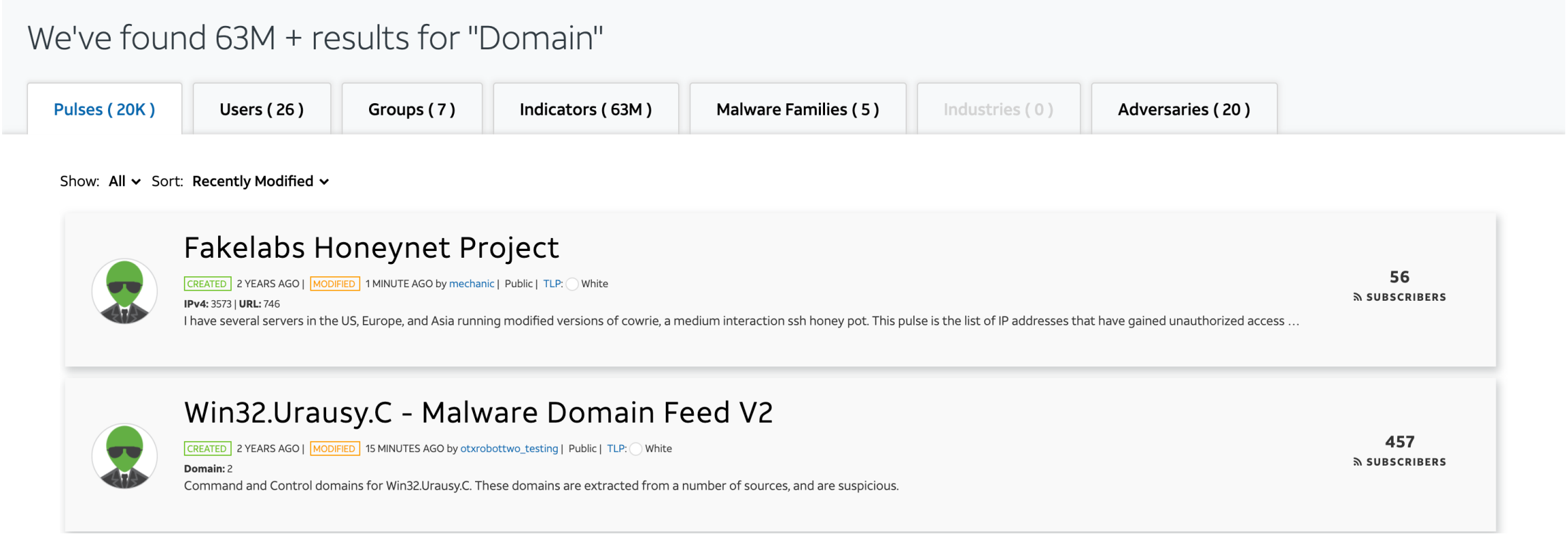


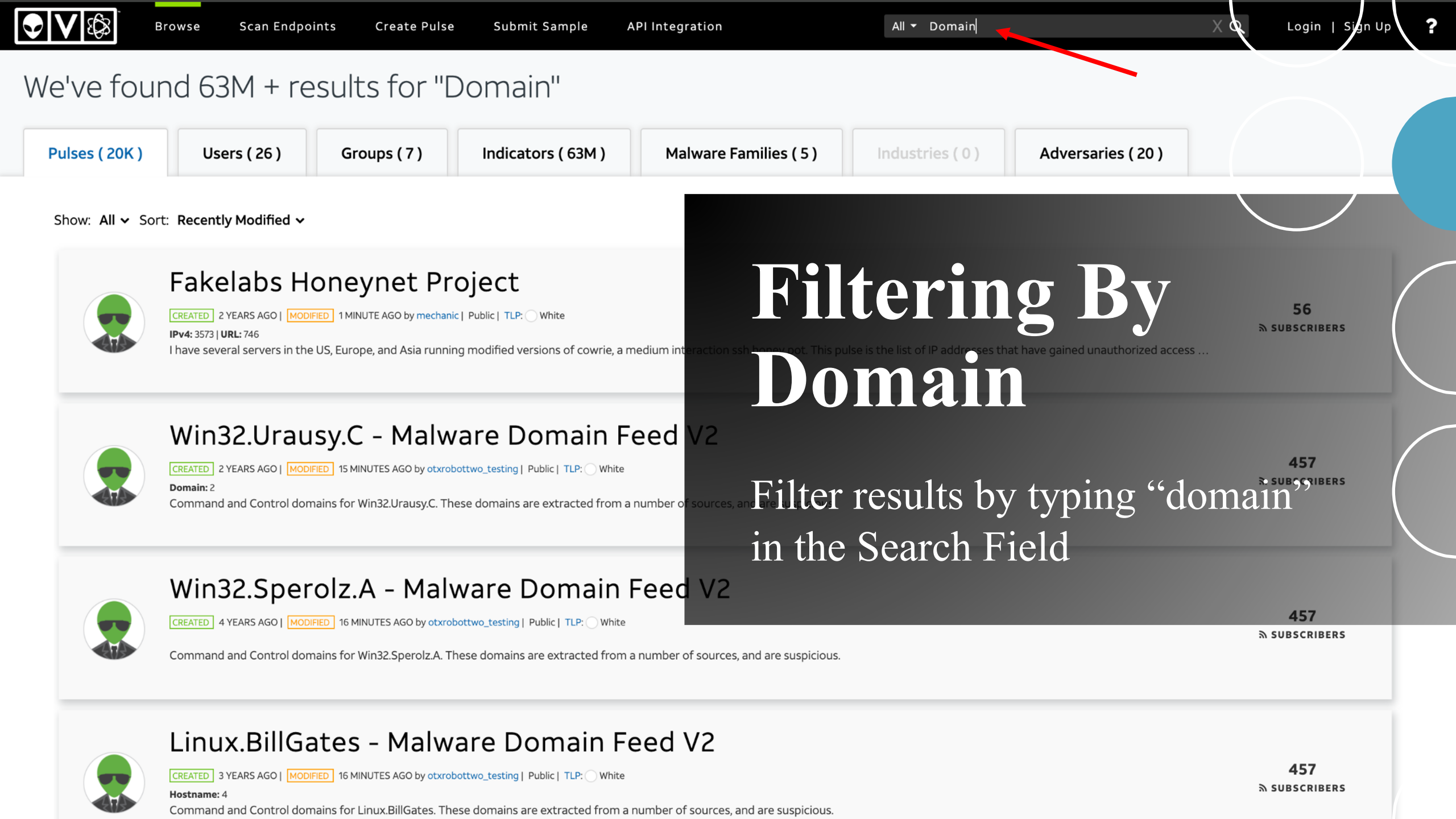
Investigating Related Pulses

Visit the Related Pulses tab to view connected IoCs.

Returning to Pulse Page

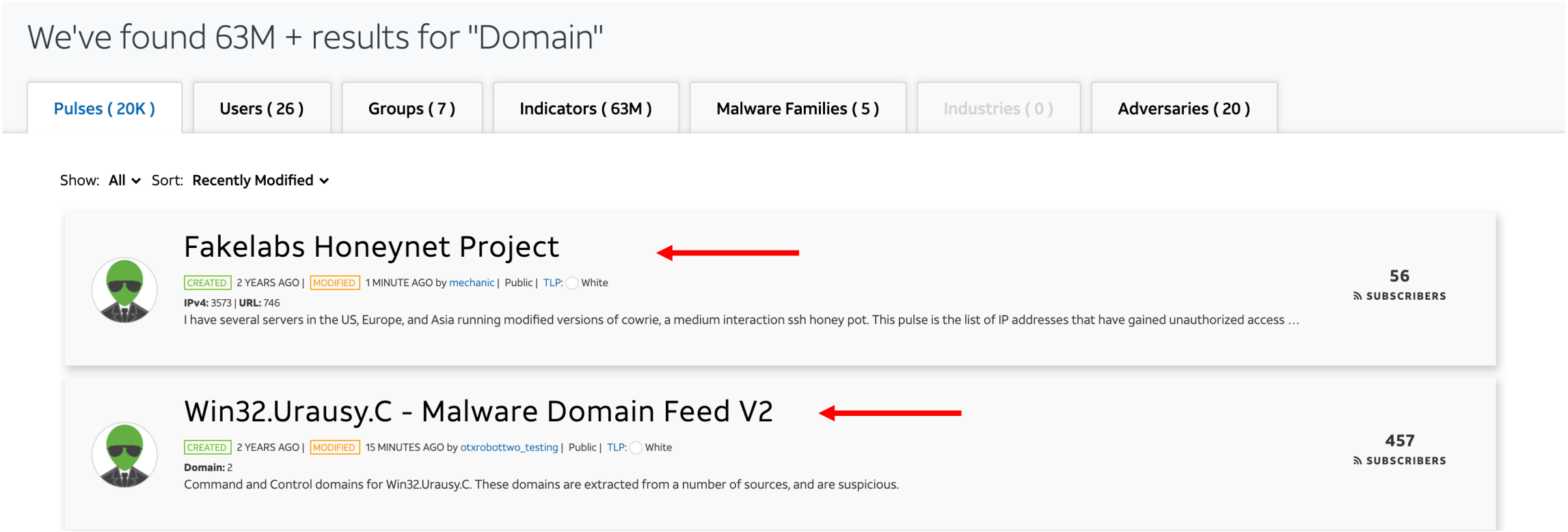
Use the back arrow in your web browser to return to the pulse page.





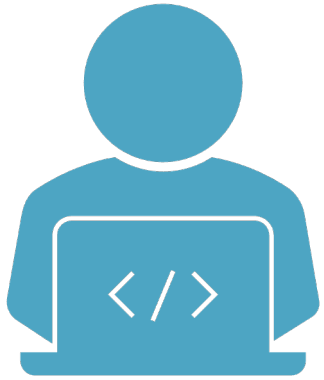
Filtering By Domain

Filter results by typing “domain” in the Search Field



Viewing Domain Indicator Details

Select a domain Indicator to view its analysis overview.



Conducting Further Searches

Search using terms like, “URL”, “IPv4”, “hostname”, and “hash”