A Lookup Tool Set for Conducting Cybercrime Investigations

Posted on July 4, 2025

Our research team has done many threat reports where we analyze published indicators of compromise (IoCs) in an effort to identify more threat artifacts or cyber resources likely associated with the threat actor infrastructure.

In one threat report, our researchers examined around 290 IoCs related to seven new threat groups listed on MITRE's ATT&CK page. This led to the discovery of more than 5,000 potentially connected artifacts that have not yet been publicized at the time. We'll use this report as an example to explain how we do it.

The process is no rocket science. Any cyber professional can conduct the same type of investigations using the right combination of tools. The starting point is typically a few IoCs, usually domain names or IP addresses. Using various internet intelligence tools, you then gather as much data as you can about those IoCs to find connected cyber resources or more information and pivot off it.

In this post, we describe the tools and the process that we rely on to produce those threat reports. It's worth noting that the methods won't give absolute certainty that the discovered artifacts are actually IoCs, but the key is to identify similarities between the IoCs and the artifacts. As more data aligns, you will have higher confidence about the potential connections.

Let's start gathering the data.

WHOIS Lookup: Finding Common Characteristics

The first step is to run WHOIS Lookup API queries for all the domains tagged as IoCs. We want to do this to get more information about the domains for two reasons. First, it will give us something

to pivot off. Second, later, when we find more potential IoCs, we can compare this information and see if there are correlations (as we've said above: the more correlations, the higher the probability that our findings belong to the same infrastructure). Here's the data we're looking to get:

- **When was the domain registered?** The likelihood of an artifact belonging to the same infrastructure as the IoC increases if they were registered on the same day, since threat actors tend to register domains in bulk.

- **Who is the registrar, and what is the name server?** The registrar would also be the same if domains were registered in bulk. The name server could also serve as a clue—although registrars often have multiple name servers, there is still a chance that the domains are connected even when they use different name servers.

- **Where is the domain registered?** Another clue we can use is the registrant country of the domains, since this data would be the same in bulk registrations.

- **Is there a public registrant email address?** While in most cases registrant emails are redacted for privacy these days, some may still be public, and we can pivot off these email addresses in the following steps.

All this information is compiled into a spreadsheet that we'll use later. APIs are convenient here because you can fill out the spreadsheet programmatically.

Historical WHOIS Lookup: Uncovering Hidden Data

Now, not all domains from the IoC list will have current WHOIS records. If there are none, the domain has likely been taken down either by law enforcement or by the threat actors after it has served its purpose.

However, these domains should not be discarded right away because their WHOIS history might be hiding useful information. For one, the registration data and registrar details missing in the current WHOIS record will be in the historical WHOIS details, which you can retrieve using WHOIS History API.

WHOIS history will also show if a domain is old and was abandoned a long time ago, but threat actors re-registered it at some point to leverage the domain's past reputation. Security systems trained to block newly registered domains (NRDs) may not flag re-registered domains.

The historical WHOIS record of a domain may also reveal a public email address that had been used in the past. That email can still be used to uncover associated domains.

Reverse WHOIS Lookup: Identifying Domain Connections

Remember the public email addresses you found in the domain IoCs' current and historical WHOIS records? You can run queries for them on Reverse WHOIS API—this lists all domains that were registered using the email addresses, either at present or historically.

One example is a Yahoo! mail used to register a domain tagged as an IoC for APT42. A reverse WHOIS query revealed that it appeared in the current WHOIS record of one domain not found on the APT42 IoC list.



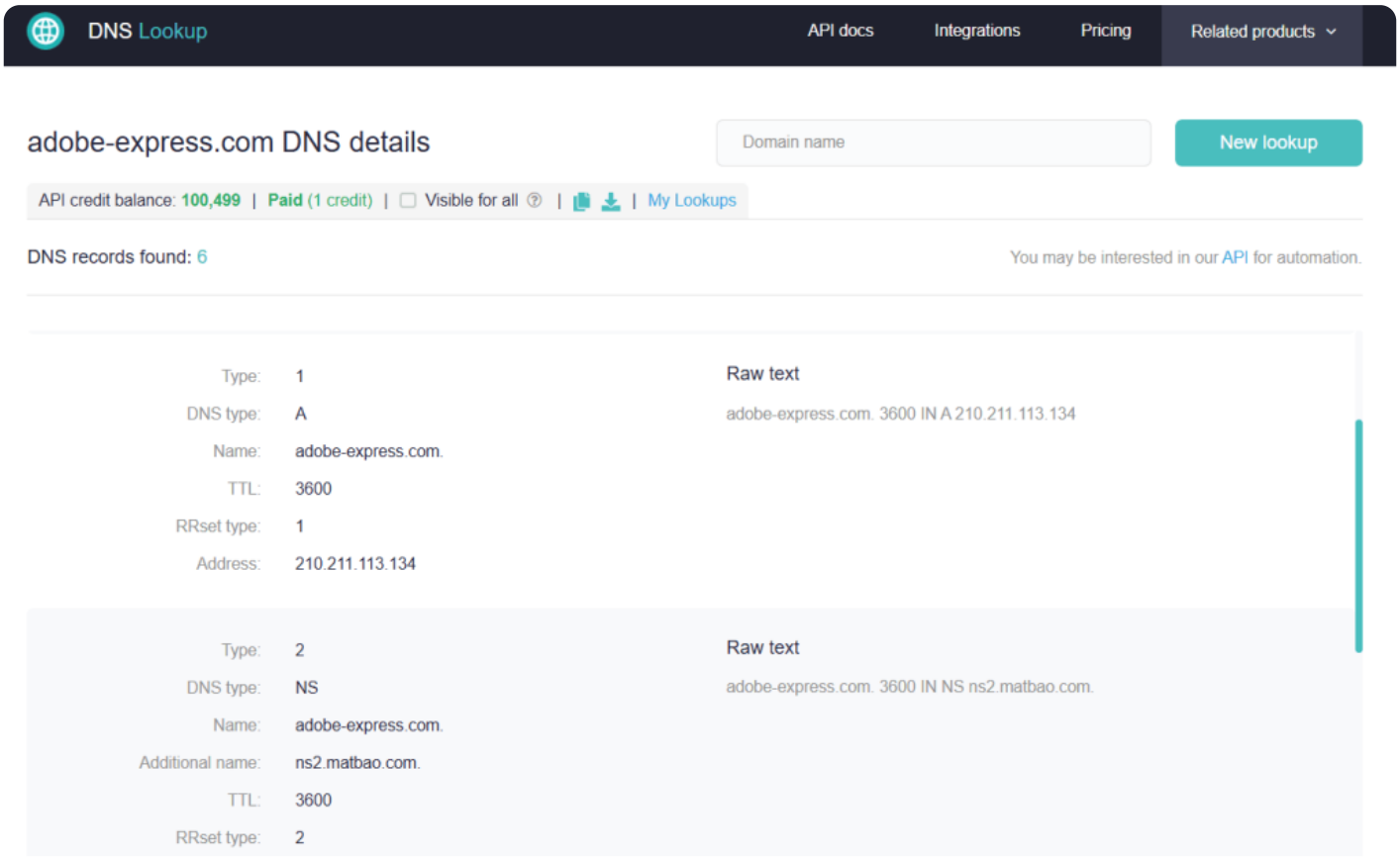
A historical reverse WHOIS query on the same email address gave us two additional domains that look quite similar to those used by APT42 but haven't been publicly listed as IoCs yet.



By the end of the reverse WHOIS queries, we usually have several domain artifacts that are associated with the IoCs through their registrant emails. We call these email-connected domains, and they are listed on the spreadsheet, along with the other WHOIS information we initially discovered.

DNS Lookup: Retrieving IP Resolutions

The next step is to run DNS lookups to see if the domain IoCs resolve to IP addresses. We use the DNS Lookup API for this. If the domains do resolve, it means that they might still be actively used.

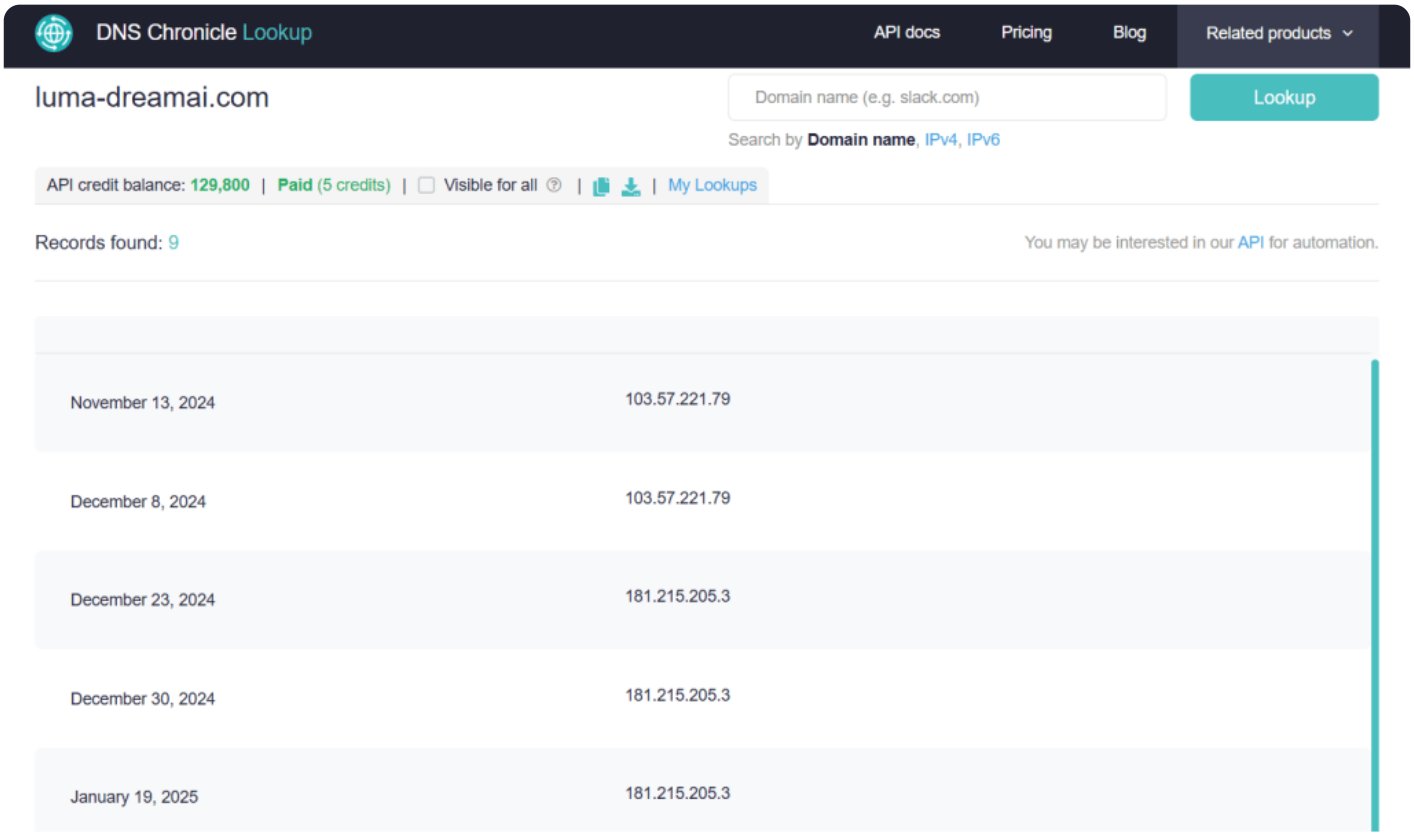


We then list all the IP addresses resolving the domains and use them later to find associated domains—those that resolve to the IP addresses but do not appear on the IoC list. It's worth noting that we usually exclude IP addresses with more than 300 connected domains, since these IPs are shared and could also be used by legitimate domains.

Historical DNS Lookup: Detecting Past IP Connections

DNS lookups give us the IP addresses *currently* resolving the domain IoCs, but some domains might not have those. As such, it's worthwhile to also look into historical IP resolutions, and for that, we use DNS Chronicle API.

The historical DNS data primarily helps us match the timelines of the DNS resolution and when the malicious campaign we're investigating was active. For instance, if the campaign was ongoing between November 2024 and May 2025, we would look closely at IP resolutions that occurred during that period for high-confidence results. We list those IP addresses and use them to find associated domains.



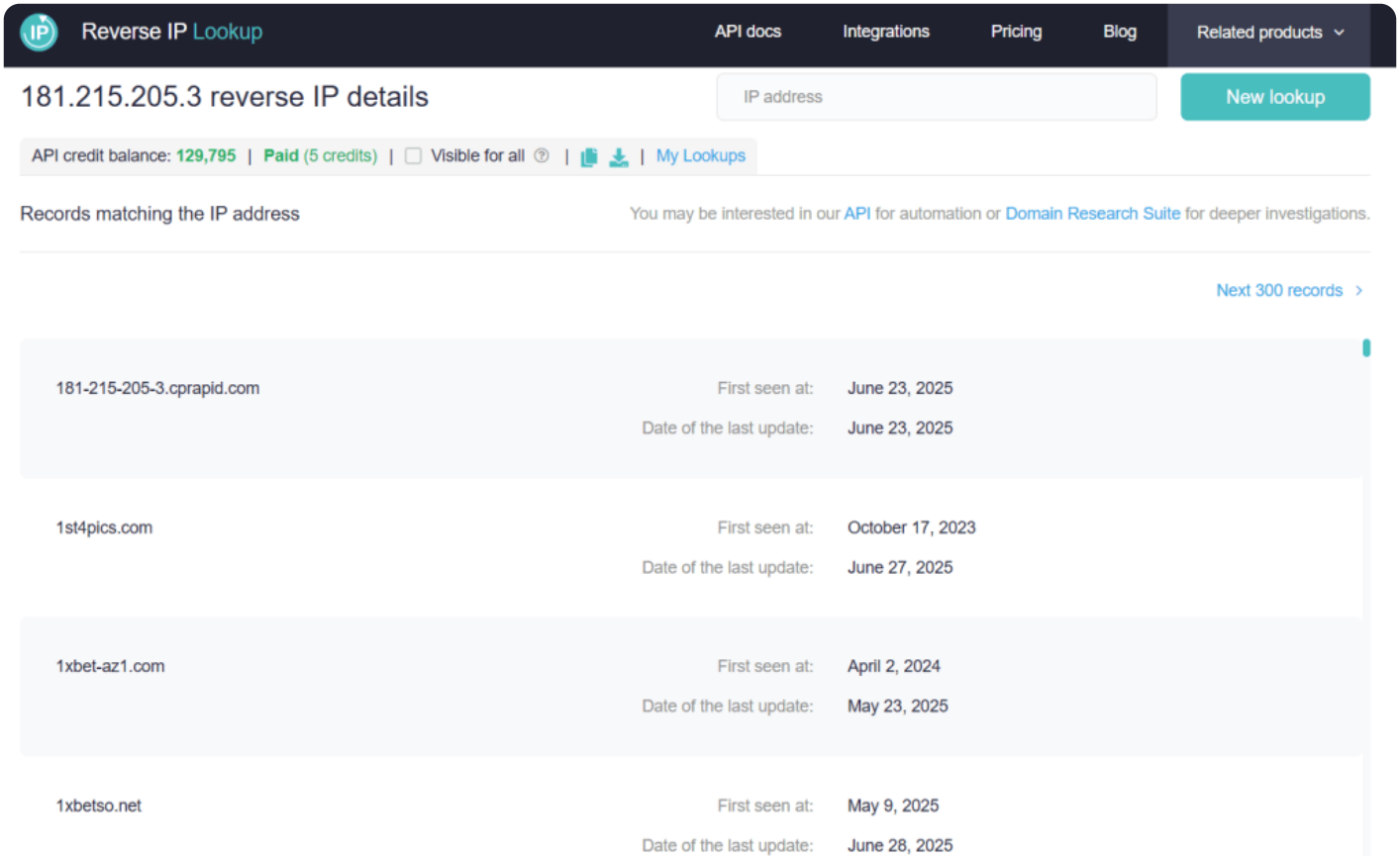
The number of past IP resolutions can also clue us in about the domain IoC's fast flux DNS network association, if any, especially when the changes occur frequently over a short period.

Reverse IP Lookup: Uncovering IP-Connected Domains

Now we have a list of IP addresses obtained from the DNS Lookup API and the DNS Chronicle API. The next step is to find what else is there on the infrastructure using Reverse IP API. This tool

retrieves all domains associated with an IP address, and to reiterate, we exclude IPs with more than 300 connected domains since they could be using shared hosting or the same CDN.

By the end of this step, we would have a list of IP-connected domains that are associated with potentially dedicated IP addresses that have resolved the IoCs. At this point, we don't really have much confidence that these domains belong to the malicious infrastructure in question – we have correlations.



To refine the list for higher confidence, you can again run WHOIS lookups for those IP-connected domains and look for similarities with the IoCs, such as in terms of registration date, registrar, and registrant country.

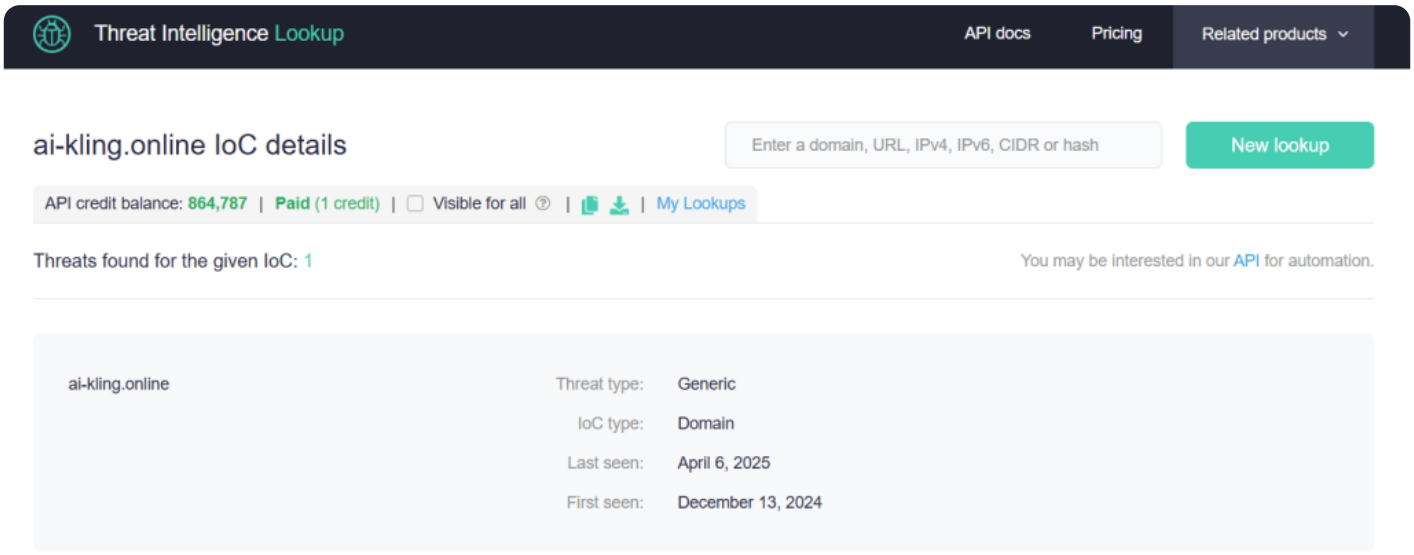
You may also run a string analysis on the IP-connected domains and pinpoint those that appear very similar to the IoCs (e.g., malicious-domain[.]com and malicious-domain[.]net)

Threat Intelligence API: Finding Proof of Malicious Involvement

At this point, we already have threat artifacts with various levels of confidence comprising:

- Email addresses used to register the domain IoCs (current or historical)
- Email-connected domains
- IP addresses resolving the domains IoCs (current or historical)
- IP-connected domains

This data is probably strong enough to upload it into security solutions so that they flag traffic to and from these IPs, but not strong enough to say, “these are also IoCs”.



What we can do at this point is run all the domains and IPs on the Threat Intelligence API to see if any are already known to be malicious. If any are, that means the other domains that share many similarities are also highly likely to be part of the attacker's infrastructure.

If some IP addresses are malicious, you can check ASN data from the DNS lookup result to see if that IP belongs to a known public cloud or shared hosting provider. If they don't, then that IP address is potentially controlled by the threat actor. That means all domains resolving to them can be considered malicious.

What Else Can You Do?

We have already gathered several threat intelligence points at this point, but there are still many more ways to pivot from the data points we've gathered to find new information – whether to increase confidence or to try uncovering new potential IoCs. Here are some examples:

- **Identify IP geolocation**: Run the domains on IP Geolocation API to see where the IP resolutions took place. This provides additional context about the attacker's infrastructure

and establishes more connections between the IP addresses.

- **Use other DNS records**: DNS Lookup API returns several types of DNS records (e.g., SOA, TXT, or CNAME) that you can pivot off using reverse DNS lookup tools to find other cyber resources using the same DNS records.

- **Find string-connected domains**: Run the text strings or words used in the domain IoCs on the Domains and Subdomains Discovery API to identify look-alike domains. You can further refine the search by limiting it to a specific period.

- **Identify victim IP records**: If you have access to NetFlow data, you can analyze requests sent to the IoCs and learn about the attack targeting and victim distribution.

- **Internal DNS traffic log match**: You can check your organization's DNS logs to see if any network traffic involves the IoCs or the connected artifacts you found.

- **Double-check maliciousness**: Run the connected domains you've identified on Virus Total to obtain additional proof and check if other engines have also detected those artifacts.

There are so many other things you can do with all the data points you've gathered — we've listed just a few. It's also important to keep timeliness in mind since threat infrastructures can change fast—dormant artifacts could be weaponized anytime, while active indicators could be dropped seconds after security solutions detect them. So, if something walks like a duck (say, has a matching registrant email) and talks like a duck (resolved to known malicious IP at some point in time), but VirusTotal or Threat Intelligence API don't tell you that it's a duck, it's probably because it hadn't hatched yet.