☰ **Open navigation**

Shodan (https://www.shodan.io/): Used by pentesters, researchers and data scientists everywhere to analyze information about computers on the Internet. From webcams to SCADA to looking at where various SSL information in certificates can tie organisations together. It is a common tool used by many different people.

TL;DR -- You can find the Shodan Transforms in the **Transform Hub**. To use all of the different Transform options (or you can stick with the free options), click on **Settings** in the **Transform Hub** after installing to add your API key.

Numerous Transforms have been written for Shodan, however, upon studying the information provided by Shodan and examining how it could be integrated into the needs of Maltego users. Her is one example:

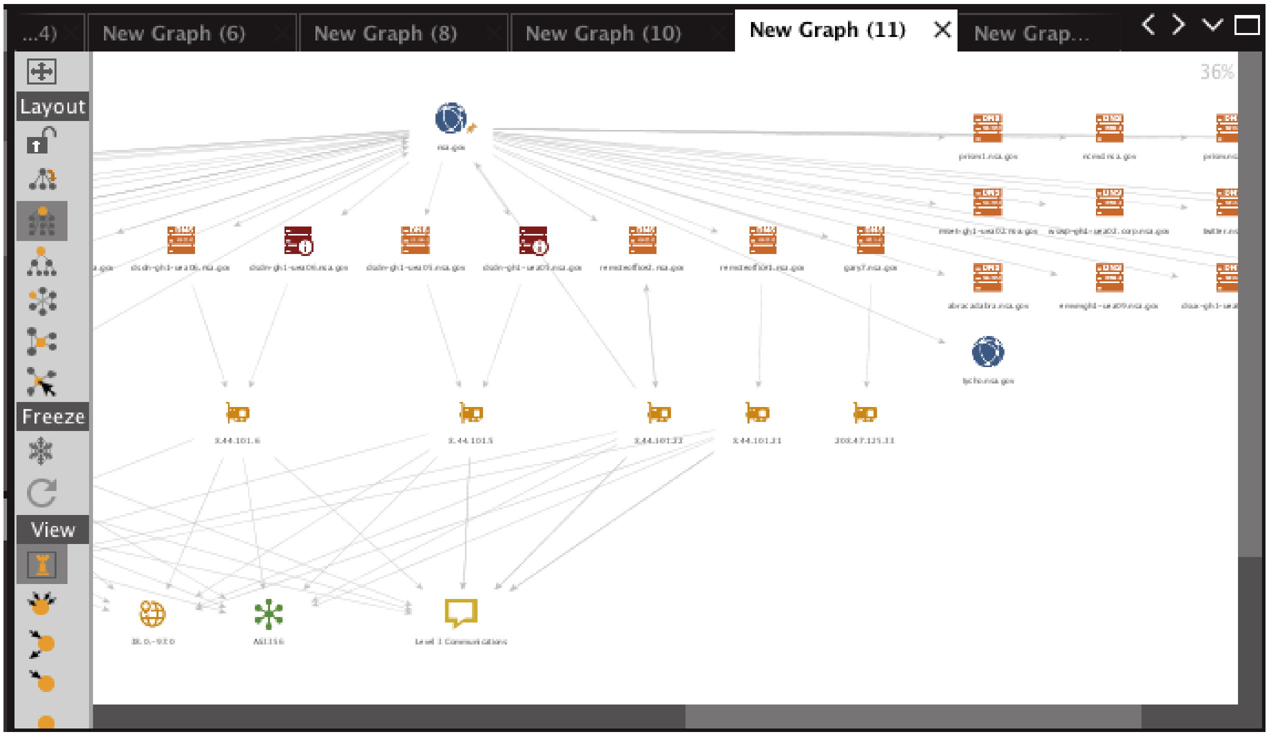
IP Information

Taking an IP address, users can identify various pieces of information for that IP address, these are broken down into the following:

- **Service -** A service is an application running on a particular port and is represented as <port>:<banner> in a new *maltego.Service* entity. If the banner is unknown the text "<unknown>" is displayed.
- **Hostnames -** Any hostnames enumerated by Shodan will be displayed. Most often this is the reverse DNS for the IP address.
- **Owner Details** - This will return two phrases (unless they are the same), one for the ISP and one for the organisation identified by Shodan.
- **Location -** If GPS and Location variables have been identified these will be returned as one or two different entities.
- **AS -** Returns the AS number for the IP address in question.

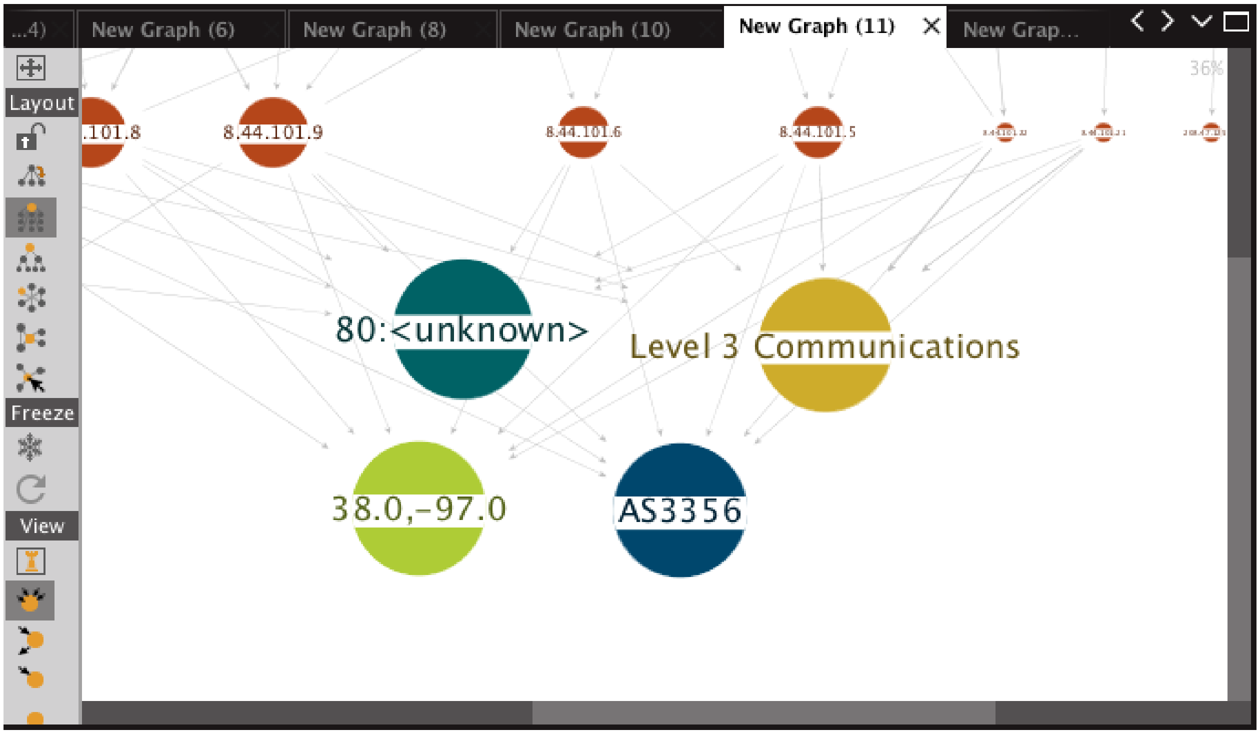
With this kind of information and the power of Maltego it means you can easily do link analysis across a large number of IP addresses (and later networks!) ... fantastically. Graphing information such as common services, owners or locations means that even if the machines you are investigating/targeting are on disparate networks you can find connection between them. It is of course still up to the analyst to identify if the connections are valid or not.

An example of this could be something like looking at the infrastructure of the NSA (starting with nsa.gov) and performing a simple footprint with Maltego (Domain -> DNS -> IP Addresses). Once we have the IP addresses we can run the "*To Shodan Details*" Transform and see the following:



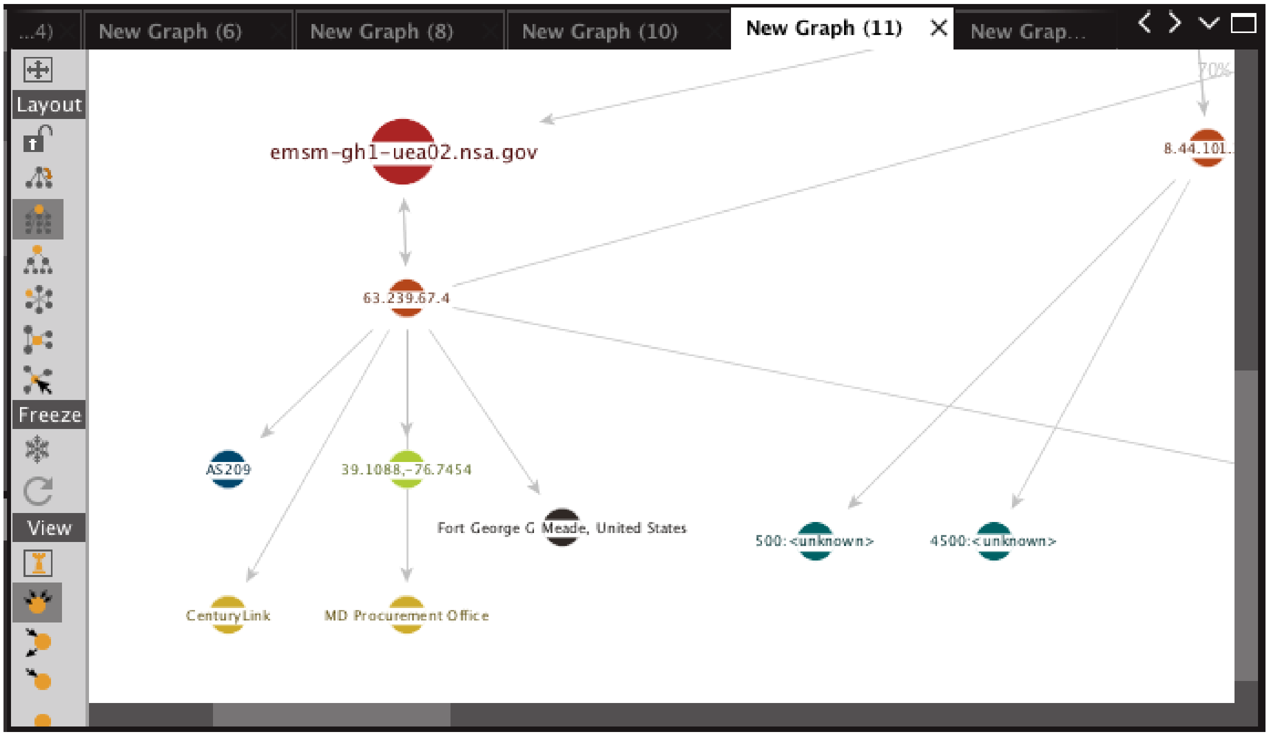
(https://2.bp.blogspot.com/-xp8mK2CN-3A/Vw-r0gVXYxI/AAAAAAAAAMM/uU1qovE0alMtYZSGS9B2vBOBhz19aWUqQCLcB/s1600/shodan1.png) (https://2.bp.blogspot.com/-xp8mK2CN-3A/Vw-r0gVXYxI/AAAAAAAAAMM/uU1qovE0alMtYZSGS9B2vBOBhz19aWUqQCLcB/s1600/shodan1.png)

From here we can switch to 'bubble view' (replaced in M4) to get an idea of the most common nodes, and we see the usual suspects, Layer 3 communications (a T1 provider), the AS used and a number of machines running what looks like webservers:



(https://4.bp.blogspot.com/-dJW5NDnl3jw/Vw-tSgUOjUI/AAAAAAAAAMo/7HaBTjxKABkyuWVqWDPzJLfo6jmsCkQlwCLcB/s1600/shodan2.png) (https://4.bp.blogspot.com/-dJW5NDnl3jw/Vw-tSgUOjUI/AAAAAAAAAMo/7HaBTjxKABkyuWVqWDPzJLfo6jmsCkQlwCLcB/s1600/shodan2.png)

Above example shows the ability to correlate - however it may be even more interesting to look at machines that did not match the more common nodes. Looking at these you can quickly identify 'the odd one out':



(https://3.bp.blogspot.com/--N9VTv0mm90/Vw-smYFh0YI/AAAAAAAAAMk/zk1L9hf9I5Q4whIZvriYZ5LalChcMJ3lwCKgB/s1600/shodan3.png)

(https://3.bp.blogspot.com/--N9VTv0mm90/Vw-smYFh0YI/AAAAAAAAAMk/zk1L9hf9I5Q4whIZvriYZ5LalChcMJ3lwCKgB/s1600/shodan3.png)

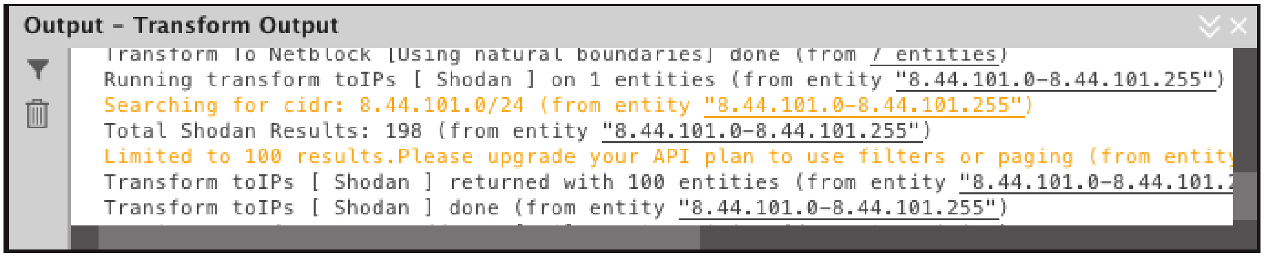
Netblocks

The ability to send a netblock to Shodan and have it return IP Addresses it has found within a particular range is phenomenally useful. As such we have included this Transforms within the pack! What it gives you is the ability to take a large network space (think multiple Class A/B's) and have only a small subset of that returned. This is usually interesting as the results returned show only the populated space in the netblock -- Shodan does the pre-scanning for you!Keeping with our previous example of the NSA, if we take a handful of IP addresses within the 8.44.101.x network space found previously:8.44.101.21 - remoteoffice1.nsa.gov8.44.101.8 - smtp.nsa.gov8.44.101.9 - smtp.nsa.gov8.44.101.5 - **dsdn-gh1-uea05.nsa.gov**

8.44.101.20 - remoteoffice.nsa.gov
8.44.101.6 - dsdn-gh1-uea06.nsa.gov
8.44.101.22 - remoteoffice2.nsa.gov

If we now run the Transform "To Netblock [Using natural boundaries]" to get the class C those are in (or do it manually), which returns 8.44.101.1-255.

From here you can run to "toIPs [Shodan]" and you will see the following in the ouput window:



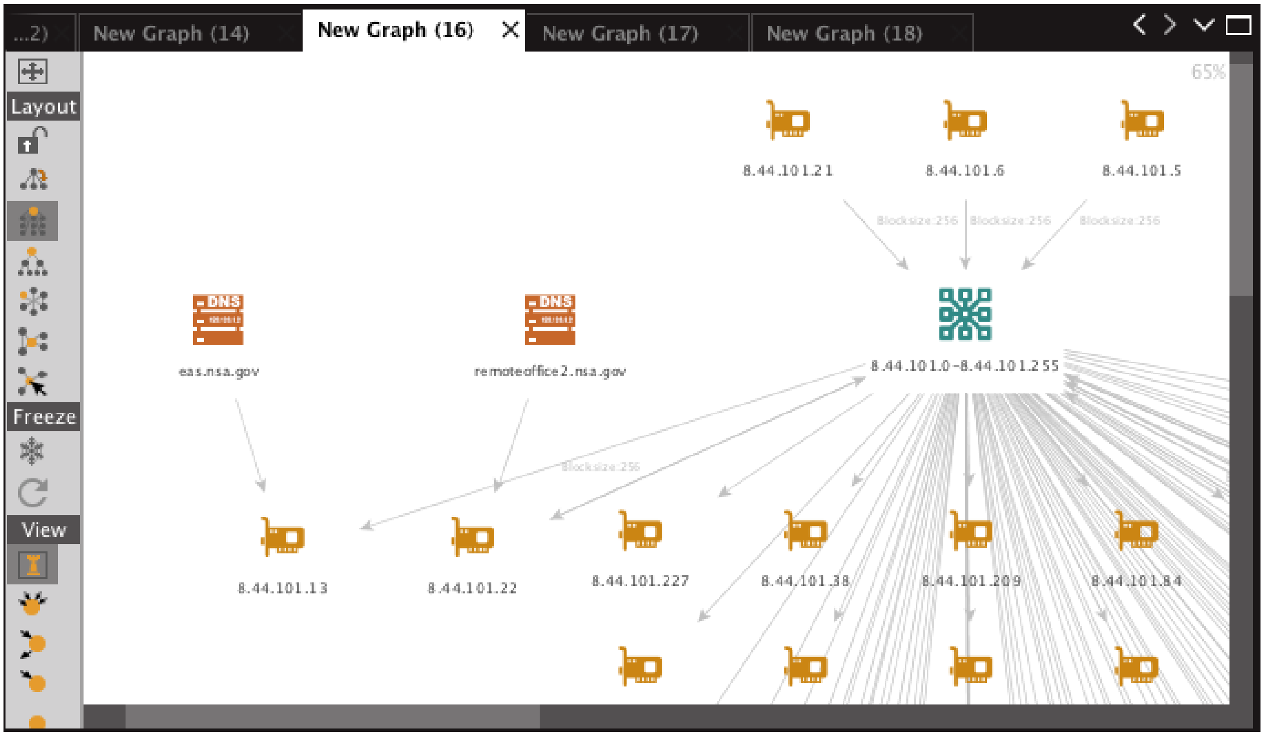
```
Transform To Netblock [Using natural boundaries] done (from 7 entities)
Running transform toIPs [ Shodan ] on 1 entities (from entity "8.44.101.0-8.44.101.255")
Searching for cidr: 8.44.101.0/24 (from entity "8.44.101.0-8.44.101.255")
Total Shodan Results: 198 (from entity "8.44.101.0-8.44.101.255")
Limited to 100 results.Please upgrade your API plan to use filters or paging (from entity
Transform toIPs [ Shodan ] returned with 100 entities (from entity "8.44.101.0-8.44.101.
Transform toIPs [ Shodan ] done (from entity "8.44.101.0-8.44.101.255")
```

(https://3.bp.blogspot.com/-t7jpE_h964M/Vw-xQd0G2TI/AAAAAAAAAM4/vJapyFZJ3J4sg__DzVIS6ozsa9bEtaj1wCLcB/s1600/shodan4.png)

(https://3.bp.blogspot.com/-t7jpE_h964M/Vw-xQd0G2TI/AAAAAAAAAM4/vJapyFZJ3J4sg__DzVIS6ozsa9bEtaj1wCLcB/s1600/shodan4.png)

As you can see from this example we're using a free API key and our results are limited to 100 but you can use your own paid-for key to get all the results available! Even with just the first 100 results (of 198) it means we have already managed to narrow down our space further.

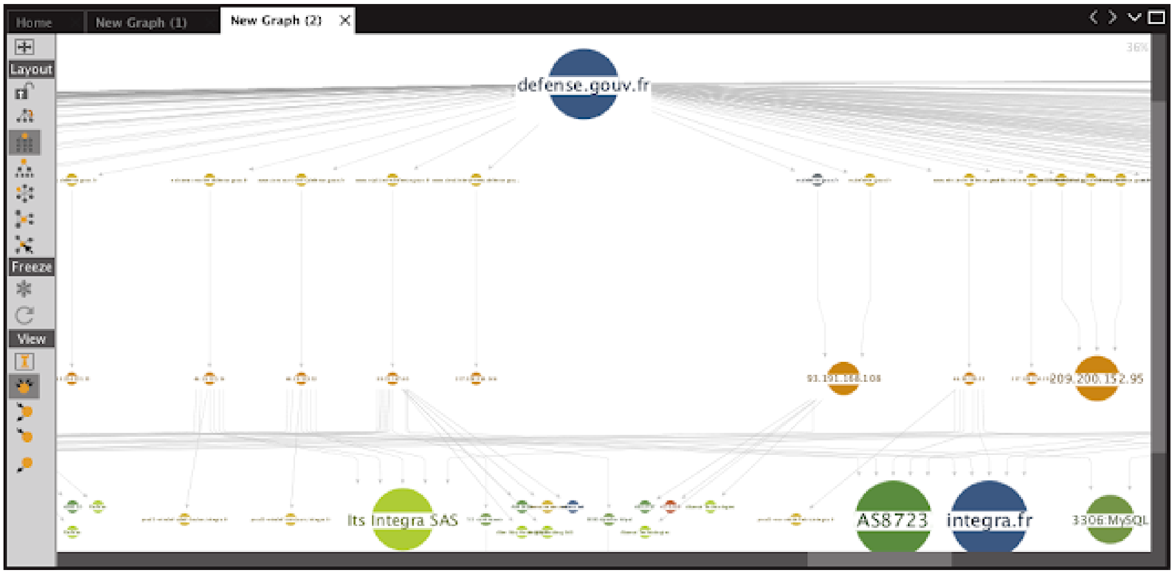
Now we can look at the results and perform tasks such as looking at the reverse DNS names (with the Transform "To DNS Name [Reverse DNS]") and already get new DNS names we previously did not find such as *emvm-gh1-uea08.nsa.gov*and *eas.nsa.gov.*



[(https://4.bp.blogspot.com/-4QAbkBYacvY/Vw-yPWt4lnl/AAAAAAAAANA/YrtjTJYf_lMzxDsAHo3KxHL6PSmqLYPKACLcB/s1600/shodan6.png)](https://4.bp.blogspot.com/-4QAbkBYacvY/Vw-yPWt4lnl/AAAAAAAAANA/YrtjTJYf_lMzxDsAHo3KxHL6PSmqLYPKACLcB/s1600/shodan6.png)
[(https://4.bp.blogspot.com/-4QAbkBYacvY/Vw-yPWt4lnl/AAAAAAAAANA/YrtjTJYf_lMzxDsAHo3KxHL6PSmqLYPKACLcB/s1600/shodan6.png)](https://4.bp.blogspot.com/-4QAbkBYacvY/Vw-yPWt4lnl/AAAAAAAAANA/YrtjTJYf_lMzxDsAHo3KxHL6PSmqLYPKACLcB/s1600/shodan6.png)

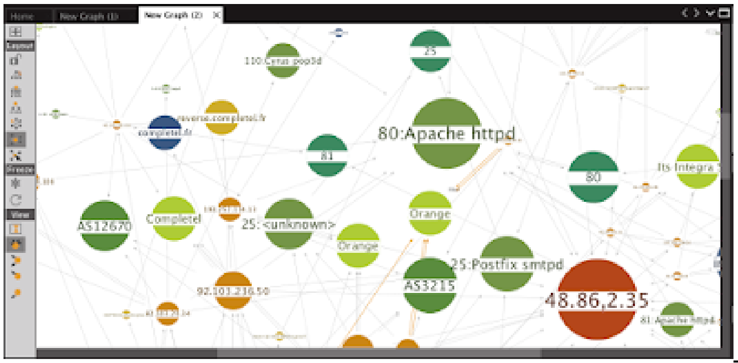
Service/Port Splitting

One thing you might notice about the first example is that there is a service entity returned that contains the details in the format of <port> : <service> . There are two additional Transforms included in the Shodan Transform Hub item that will break these apart into the various ports and services. This allows you to quickly visualize which ports and applications are more commonly used.If we look at an example quickly mapping *defense.gouv.fr* to DNS, then to IP addresses as we did above we see something like the following:



(https://3.bp.blogspot.com/-D1z4HR1e_IQ/VxY4y6DiHwI/AAAAAAAAAOU/_6X0Q33EjtMC3oS8CulccmgmU4WWbm7HwCLcB/s640/shodan12.png) (https://3.bp.blogspot.com/-D1z4HR1e_IQ/VxY4y6DiHwI/AAAAAAAAAOU/_6X0Q33EjtMC3oS8CulccmgmU4WWbm7HwCLcB/s1600/shodan12.png)

From here however it becomes more interesting as we can take each of the services to a port and banner and within bubble view examine the common infrastructure on a port and service level:

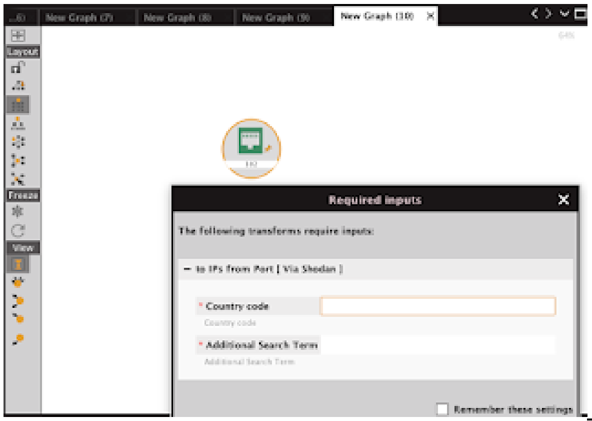


(https://2.bp.blogspot.com/-2LkWs7tSOT8/VxY4y-CXn6I/AAAAAAAAAOY/lBahtK1fZwMwjvC3cD7aHY4WXlvatg_7ACKgB/s400/shodan13.png) (https://2.bp.blogspot.com/-2LkWs7tSOT8/VxY4y-CXn6I/AAAAAAAAAOY/lBahtK1fZwMwjvC3cD7aHY4WXlvatg_7ACKgB/s1600/shodan13.png)

Typically you would see something like the graph above where there are a lot of port 80's running an HTTP of some kind, but it is interesting to see things like port 81,82,83 and 84 as well. In this case these all seem to be a standard webmail configuration. A graph like the one above however is filled with additional interesting artifacts.

Further Port Manipulation

From a port entity (either in your existing graph or dragging it in from the palette) you can also run Transforms that identify other IP addresses running services on that port. For example if we look at S7 devices (from **https://icsmap.shodan.io/** (https://icsmap.shodan.io/)) we can see that they generally run on port 102.In Maltego we add the port to our graph and run the Transform to *IPs From Port [via Shodan]*. This gives us the option of adding additional terms in the query (that might be found in the response) as well as the country code as seen below:



Required inputs

The following transforms require inputs:

– to IPs from Port [Via Shodan]

* Country code

Country code

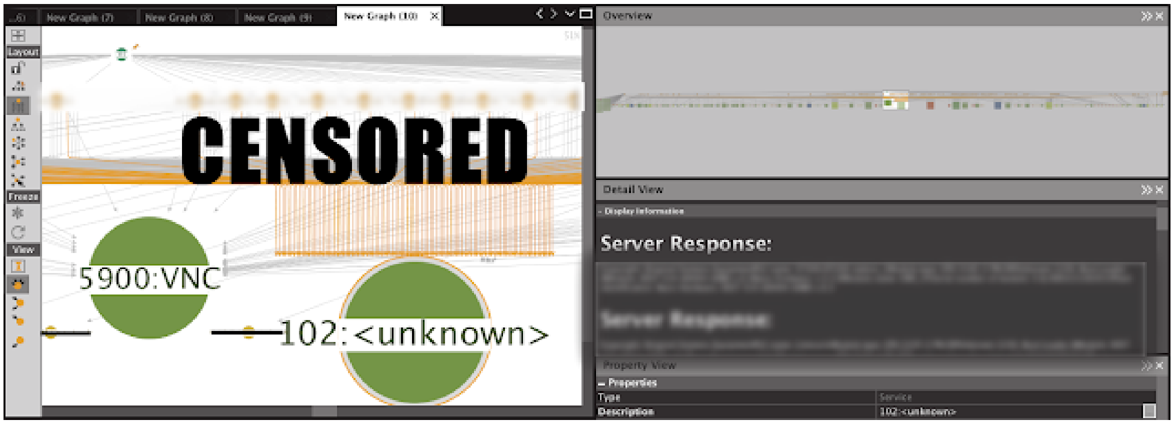
* Additional Search Term

Additional Search Term

□ Remember these settings

(https://1.bp.blogspot.com/-4hwB-YKsw3U/VxZJjH4K67I/AAAAAAAAAPY/K0PQzrSTnjMnzbJA6a58ghcO3l3eDykxACLcB/s320/shodan17.png) (https://1.bp.blogspot.com/-4hwB-YKsw3U/VxZJjH4K67I/AAAAAAAAAPY/K0PQzrSTnjMnzbJA6a58ghcO3l3eDykxACLcB/s1600/shodan17.png)

From here we get a number of results back for IP addresses that have services running on port 102. We can then take each of these services to the details for those IP addresses and visualize the results to identify commonality between them. Here we can see that a lot of the machines running the Siemens S7 devices on port 80 also have VNC listening on port 5900.



Display Information

Server Response:

Property View

– Properties

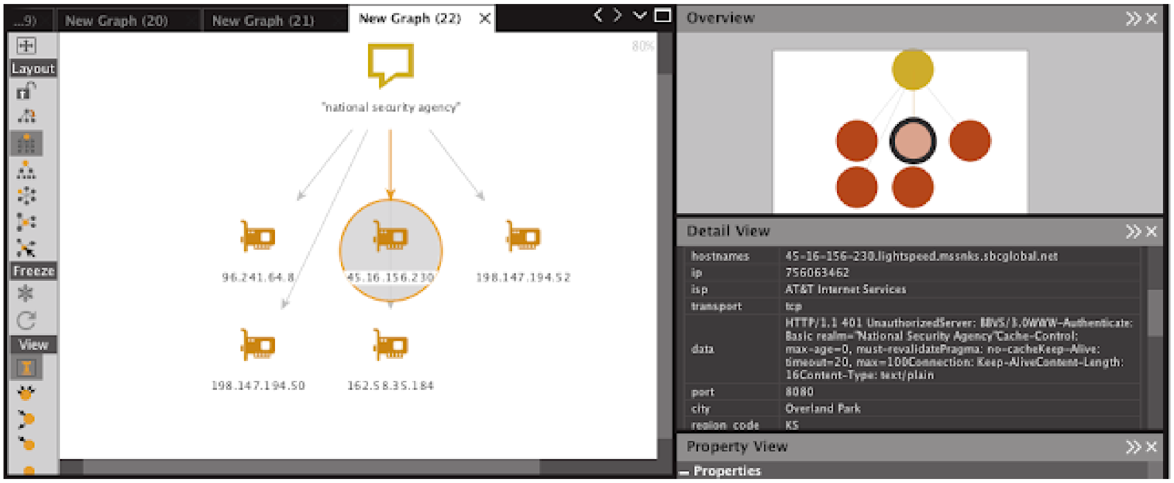
Type	Service
Description	102:<unknown>

(https://4.bp.blogspot.com/-MoBSpZ_Ip9M/VxZJR2myxqI/AAAAAAAAAPU/z7j2DzhGAc8KD0CVLQJGd1ae5Dp6OGhagCLcB/s640/shodan18.png) (https://4.bp.blogspot.com/-MoBSpZ_Ip9M/VxZJR2myxqI/AAAAAAAAAPU/z7j2DzhGAc8KD0CVLQJGd1ae5Dp6OGhagCLcB/s1600/shodan18.png)

Native Shodan Queries

In addition to the above queries we have also included the ability to search for your own custom terms or use a more guided version of the Transform.

The first is the advanced search - this Transform will send the terms you specify in a phrase entity directly and unmodified to Shodan. For example if you started with the phrase "National Security Agency" and wanted to see all results that contained that exact string you could run the "*to IPs via Shodan [Advanced Search]*" Transform. This would return the following:



Detail View

hostnames	45-16-156-230.lightspeed.mssnks.sbcglobal.net
ip	756063462
isp	AT&T Internet Services
transport	tcp
data	HTTP/1.1 401 UnauthorizedServer: BBVS/3.0WWW-Authenticate: Basic realm="National Security Agency"Cache-Control: max-age=0, must-revalidatePragma: no-cacheKeep-Alive: timeout=20, max=100Connection: Keep-AliveContent-Length: 16Content-Type: text/plain
port	8080
city	Overland Park
region_code	KS

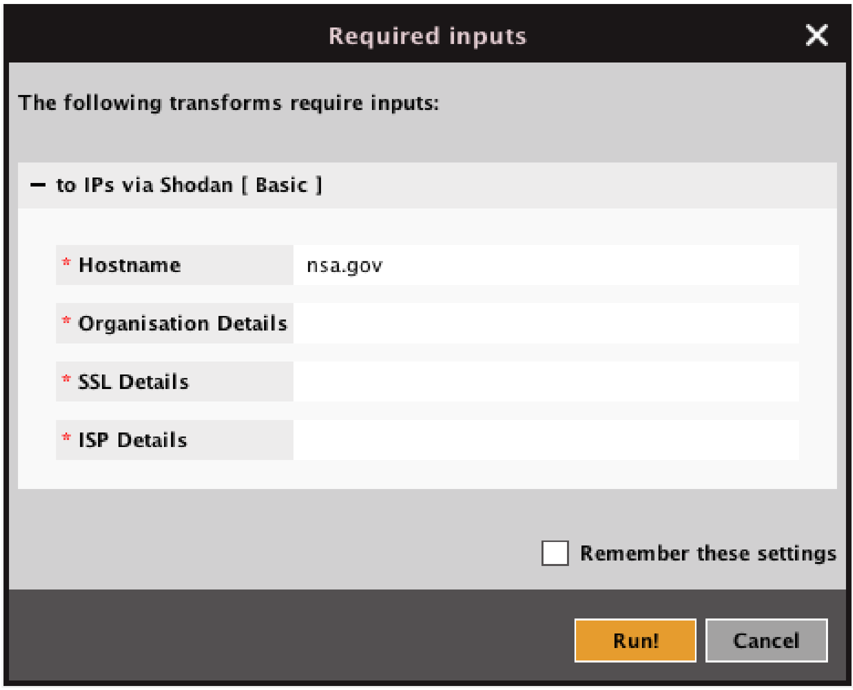
(https://3.bp.blogspot.com/-Jm-Jm45GutU/Vw-3IQSLysI/AAAAAAAAANQ/vfGN9K7t68c9Sr9M-vx2zL7FanD-lVl8wCKgB/s640/shodan7.png) (https://3.bp.blogspot.com/-Jm-Jm45GutU/Vw-3IQSLysI/AAAAAAAAANQ/vfGN9K7t68c9Sr9M-vx2zL7FanD-lVl8wCKgB/s1600/shodan7.png)

You can also see in the detail view that the text **Basic realm="National Security Agency"** is seen within the IP address highlighted. You can view additional key terms used by exploring the Shodan API documentation at **https://developer.shodan.io/api** (https://developer.shodan.io/api) and viewing the keywords available under the **/Shodan/Host/Search** heading.

If you would prefer to be guided through the four terms we use (ssl, hostname, org and isp) you can run the Transform "*to IPs via Shodan [Basic]*" which will allow you to specify the terms you want. You can use a space (" ") for terms you wish to exclude.

```
Note: The free API will only allow you to use one term at a time. To use more terms you need your own API key.
```

Let's see how this works. If you used the phrase "NSA Search" (remember this can be anything as we are doing the basic search), and you filled in the terms as shown below when running the Transform "*to IPs via Shodan [Basic]*":



The following transforms require inputs:

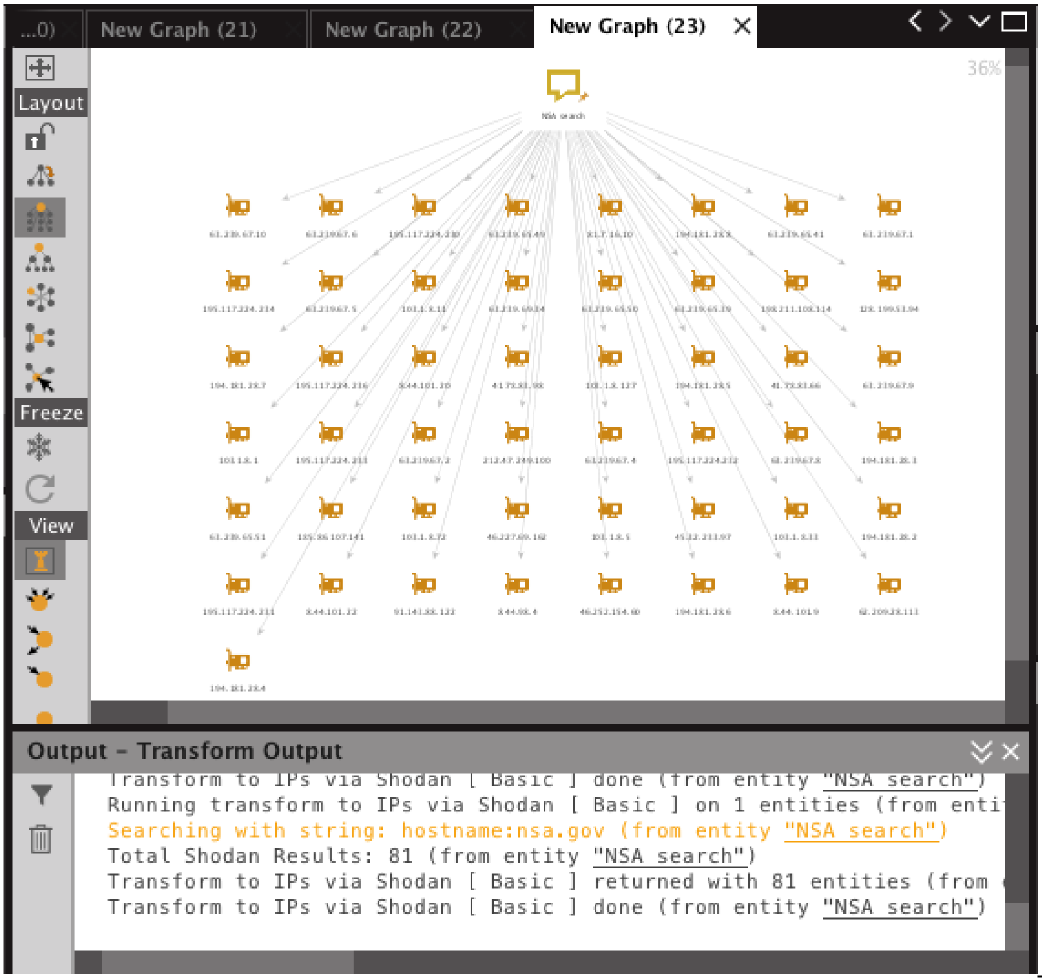
− to IPs via Shodan [Basic]

* Hostname	nsa.gov
* Organisation Details	
* SSL Details	
* ISP Details	

□ Remember these settings

(https://4.bp.blogspot.com/-jK8ej_bKuZc/Vw-40t_f96I/AAAAAAAAANc/gPBNVbX-2fgbPd_1YpYI4CJ4JcG9A_AgwCLcB/s1600/shodan8.png) (https://4.bp.blogspot.com/-jK8ej_bKuZc/Vw-40t_f96I/AAAAAAAAANc/gPBNVbX-2fgbPd_1YpYI4CJ4JcG9A_AgwCLcB/s1600/shodan8.png)

You would receive the following in your response:



```
Transform to IPs via Shodan [ Basic ] done (from entity "NSA search")
Running transform to IPs via Shodan [ Basic ] on 1 entities (from enti
Searching with string: hostname:nsa.gov (from entity "NSA search")
Total Shodan Results: 81 (from entity "NSA search")
Transform to IPs via Shodan [ Basic ] returned with 81 entities (from 
Transform to IPs via Shodan [ Basic ] done (from entity "NSA search")
```

(https://1.bp.blogspot.com/-xmXjzVfuOZ0/Vw-5DLZ5TMI/AAAAAAAAANg/v8Gqvh9Ji4s2aRbpAOZZgqpcv8jb7YR_QCLcB/s1600/shodan9.png) (https://1.bp.blogspot.com/-xmXjzVfuOZ0/Vw-5DLZ5TMI/AAAAAAAAANg/v8Gqvh9Ji4s2aRbpAOZZgqpcv8jb7YR_QCLcB/s1600/shodan9.png)

Here you can now run the standard IP to Shodan details to get the details of each of these IP addresses, and as we were searching for any DNS Name containing nsa.gov we get the following out:

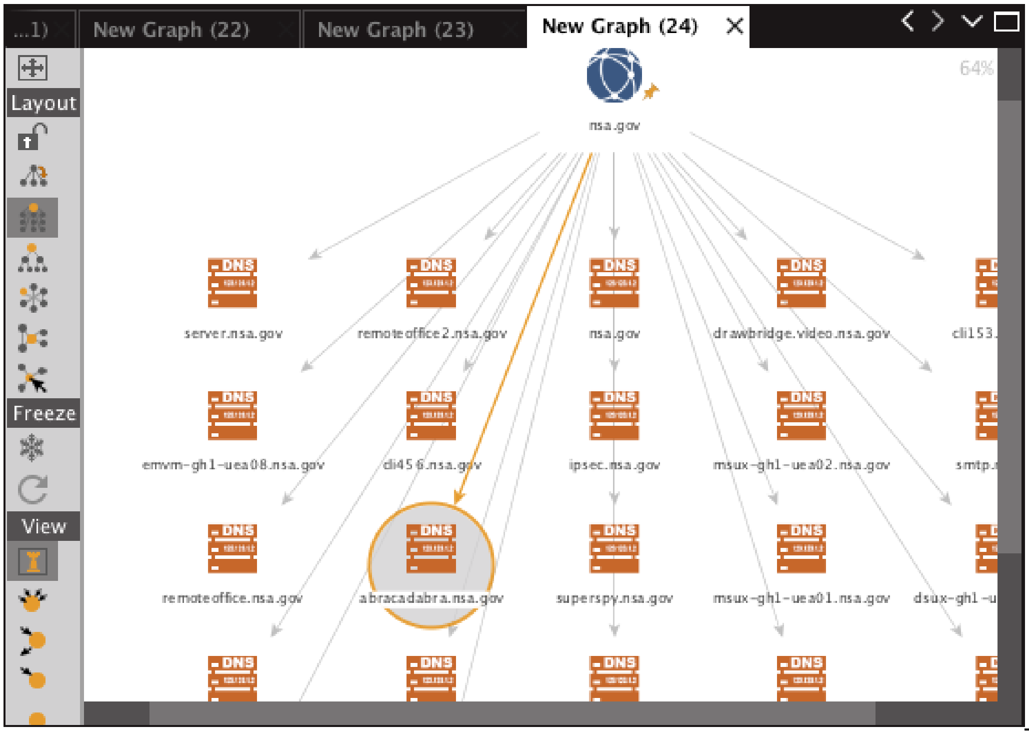
nsaoa.**nsa.gov**.cn
msux-gh1-uea02.**nsa.gov**
ns2.**nsa.gov**.cn
cli456.**nsa.gov**
emvm-gh1-uea09.**nsa.gov**
(http://www)**www.nsa.gov.pl** (http://www.nsa.gov.pl)
...list truncated...

Keep in mind that Shodan returns *anything* that contains the word **nsa.gov** - so entries like nsaoa.**nsa.gov**.cn are also returned!

Domain Queries

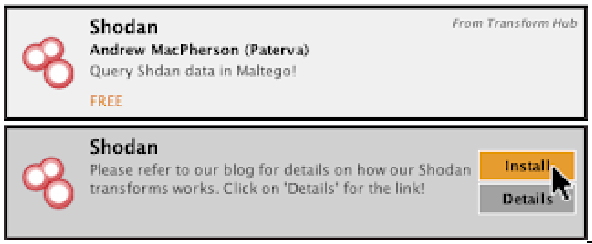
The last two Transforms are more an incorporation of the previous ones where we will use two specific Shodan keywords (namely 'ssl' and 'hostname') to search through any results found for additional DNS records that we might not have seen before using the other DNS transforms. These are very useful, especially with certificates (the SSL keyword) to find specific machines on the Internet.

If we run the two Transforms we get a nice subset of DNS names (that we had also seen before) with just two simple Transforms (*To DNS Names [Via Shodan]*and *To DNS Names SSL [Via Shodan]*) -- Abracadabra!



(https://2.bp.blogspot.com/-LaDkoT9qQ1o/Vw-7uBs7kIl/AAAAAAAAANw/YXjfl2z_Gd02VLnhxfQsNLyEqZTwOJQJQCLcB/s1600/shodan10.png) (https://2.bp.blogspot.com/-LaDkoT9qQ1o/Vw-7uBs7kIl/AAAAAAAAANw/YXjfl2z_Gd02VLnhxfQsNLyEqZTwOJQJQCLcB/s1600/shodan10.png)

Adding Shodan Transforms:
To add the Shodan Transforms it's as simple as going to the Transform Hub item and clicking on "Install":


Shodan
Andrew MacPherson (Paterva)
Query Shdan data in Maltego!
FREE
From Transform Hub

Shodan
Please refer to our blog for details on how our Shodan transforms works. Click on 'Details' for the link!

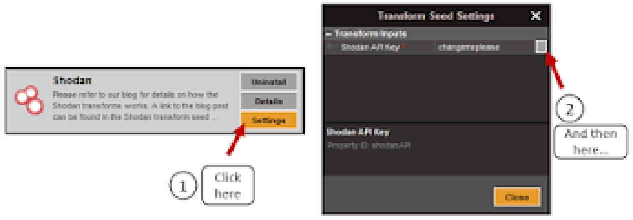
(https://1.bp.blogspot.com/-pfa0Moyajd0/VxD_nztlC3I/AAAAAAAAAOA/hynt7ye-r708W_0sih1wxDvXDFd7vq2bwCLcB/s320/shodan11.png) (https://1.bp.blogspot.com/-pfa0Moyajd0/VxD_nztlC3I/AAAAAAAAAOA/hynt7ye-r708W_0sih1wxDvXDFd7vq2bwCLcB/s1600/shodan11.png)

API Keys: Shodan API keys are free with limitations for any user on the **Shodan website** (https://www.shodan.io/) and registration is completely free.
The limitations of the free API key are as follows:

- Only the first 100 results per query
- Advanced keywords can only be used one at a time (ie you cannot search for a DNS name within a particular country).

Registered users (a once off fee) do not have these limitations (apart from a certain number of lookups per month on a registered key) and the project is really useful so we would encourage you to signup.

To add your API key click on **Settings** within the Transform Hub and enter your API key.



Shodan

Please refer to our blog for details on how the Shodan transforms works. A link to the blog post can be found in the Shodan transform seed ...

Transform Seed Settings

Transform Inputs

Shodan API Key * changemeplease

Shodan API Key

Property ID: shodanAPI

(https://2.bp.blogspot.com/--CChaZWgJkU/VxZEY2FaxTI/AAAAAAAAAPA/FMsvPG9c2q0zM2bZx7D9__2EiaV3gemkACK4B/s400/IMG_19042016_155634.png) (http://2.bp.blogspot.com/--CChaZWgJkU/VxZEY2FaxTI/AAAAAAAAAPA/FMsvPG9c2q0zM2bZx7D9__2EiaV3gemkACK4B/s1600/IMG_19042016_155634.png)

← Previous: Use Cases > Network footprinting with Maltego (https://docs.maltego.com/support/solutions/articles/15000035745-network-footprinting-with-maltego)Next: Trumpworld table to Maltego graph → (https://docs.maltego.com/support/solutions/articles/15000012033-trumpworld-table-to-maltego-graph)

Search all Maltego Guides: